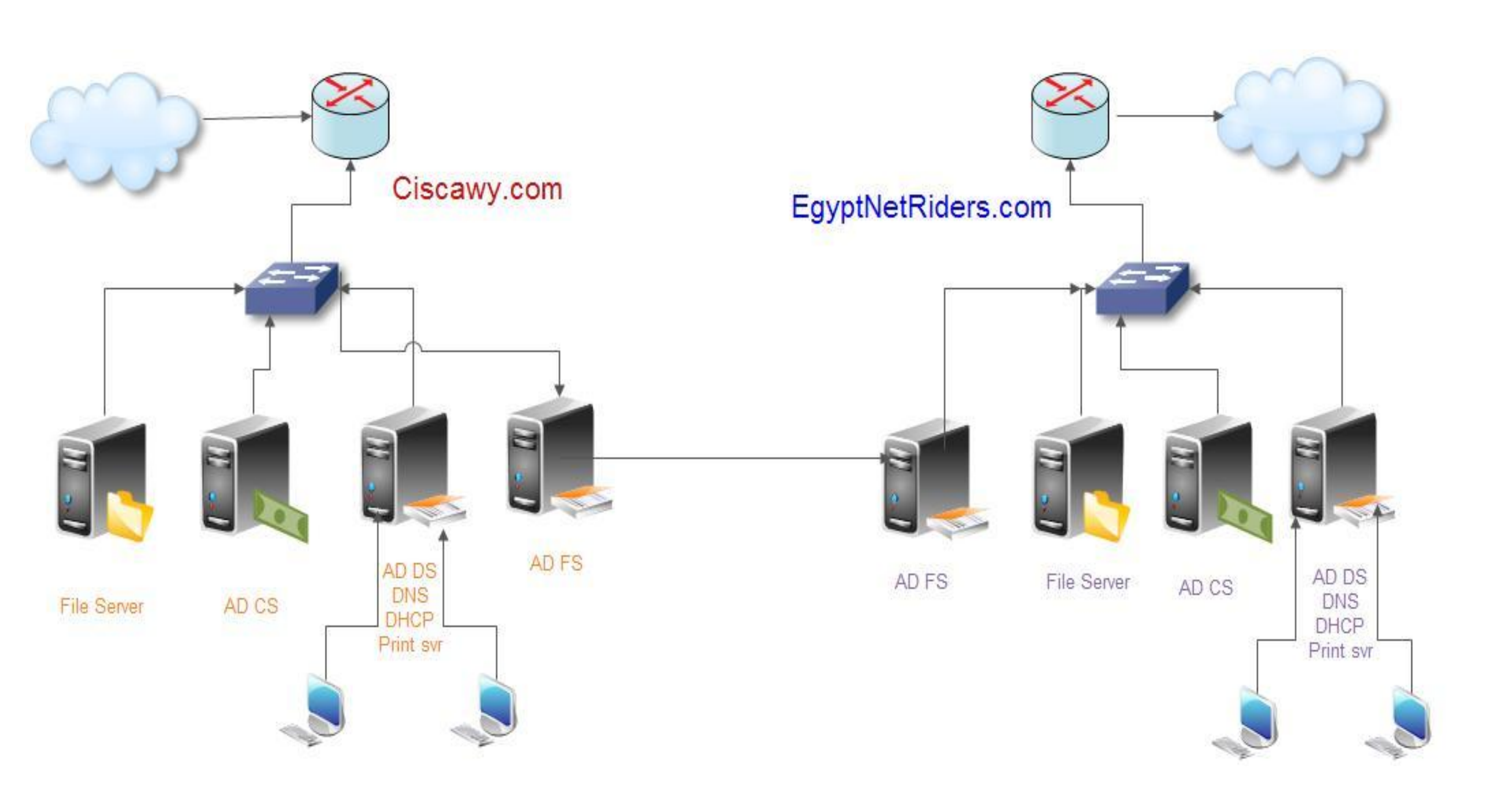
70 - 640

Configuring Windows Server 2008 Active Directory



مقدمة : -



اصبحنا في مجتمع اساسه تكنولوجيا المعلومات واصبحت الحاجة لتعلم هذا المجال مستمرة

انطلاقا بما مر بي من صعوبه في الحصول علي معلومة كاملة باسلوب صحيح وعدم وجود مواد تعليمية سهله في مجال تكنولوجيا المعلومات باللغه العربية لتسهيل المذاكرة او تسهيل الحصول عليها

وحمدا لله علي ما وصلت اليه وحرصا مني علي كل من يريد التعلم الصحيح وتوصيل المعلومة بشكل جيد وكامل

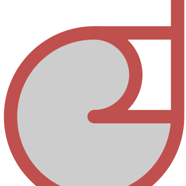
وان زكاه العلم هي اخراجه وان يكون هذا صدقة جارية لي فيما بعد

وكإحدي اهم ركائز واساسيات شركة ايجيبت نترايدرز وهي زيادة المحتوي العربي في مجال تكنولوجيا المعلومات وتقديم المعلومه باسلوب صحيح علي يد خبراء في هذا المجال

واصبح من العادي ان كل شئ بمقابل ولكن من أهم المبادئ التي تأسست عليها الشركة هي نشر العلم لكل الناس وتوفير الفائده والمعلومة لكل الناس

فكرنا في ان نقوم بتأليف المواد علمية باللغة العربية تسهيلا علي من يريد التعلم واصدارها بشكل مستمر دوري في كل ما يتعلق بمجال تكنولوجيا المعلومات وبالأخص مجال تخصصنا وهو الشبكات

سيكون هذا هو اول كتاب وسيكون هو بداية انطلاقة جديده لشركة ايجيبت نترايدرز **تحت مسمي**
Egypt NetRiders | Press



About:-

About Author:-

Eng.Basem Hamed

- Network and Information Security Engineer
- Working in Egypt NetRiders Company
- Specializing in Microsoft Networks
- Interested in Cisco and Juniper
- Editor inCiscawy Blog
- Certified:-
  MCSE, MCITP EA
  CCNA, CCNA Sec, CCNP R&S
  CEH, CISM
  JNCIA _ JUNOS
  RHCE
  CWNA

✆01001582348

About Company;-

Egypt NetRiders

- Integrated Network Solutions. Specialized in Networks and Information Security Solutions
- As a specialized company we focus on Networks and Information Security Solutions.
- We provide Two Basic Services:
  - Training courses in Network companies like Cisco, Juniper , Microsoft and CompTIA
  - Network Solutions like Analysis of Huge Networks, Design Network Topologies and Network Security.

✆0507487156 _ 01150505639
http://www.egyptnetriders.com/
FB/**EgyptNetRiders**
Twitter/**EgyptNetRiders**
http://ciscawy.com/blog/

This Book is Powered By:-



Index

- 1st Book ……………………… …………………………………………...……5
- INTRO ………………………………… ..……………..… …… …………… 6
- Preparing to Install Active Directory ……………… ………… ……… ……. 7
- Haw to join a physical computer to domain? ……… ………………..…… ….. 14
- Types of AD DS Objects ……………………… ………………... …… ….. 16
  - Different between computer and user Account!! … ……… . …. ………… ….. 17
  - Computer account ………… . …………………… ………………… …… ... 17
  - User account …………… ………… . ……………………………… … . 18
  - Groups VS Organization unit ……. . ……………………………… … … 23
  - Groups ……… ……….. ……………… …… ….. …………… …… ….. .25
  - Group Type……………………. …….. ……………… ……… …… … 25
- Forest, Tree, domain ……….. ……….. ……… ……………… … ……….. 31
  - Additional domain …… . . ……………. ……….. …….. ……………… ….. 33
  - "RODC" …………………… …….. ……. . ………………………… .. 38
  - Child Domain ……….. . …….. ……. ……… ………………………...50
  - Tree Root ………………. …… ……… …………….. ………………….. 54
- Active Directory Partition …. . …… … ……… …………………… . …..…. 59
- FSMO Roles ……………….. . ………… ……….. …… ………….…… . 64
- Active Directory Sites and Replications ……. . ..… … ……….. ……………..… 70
- Trust ………………………….. .. …………………………………..….77
- Group Policy …………………….. .. ……………………………………….79
  - Deploy Software …………….. .. ………………………………………… 87
  - Restricted Groups …………….. .. …………………………..………… 91
  - Security in Group Policy ……………. . .. ………………………………… 93
  - Group Policy Template ……………….. .. ……………………..……………104
- Backup & Restore …………………...…….. .. ………………..……………... 110
- 2ND Book ………………………….. .. ………… …………………...…. 119
- Active Directory Certification Authority …………. …. … …… …………….. 120
  - Certification…………………………….. .. ……………. … ……………. 121
  - Installing Certification Services ……….. .. ……………… ………….. . . … 122
  - KRA ……………………………….. .. …… ………………………..… 154
- Active Directory Rights Management Services ……… ……... .. ..………………176
- Active Directory Federation Service ……………….. .. .. …………………... …195
  - Install Federation Service ……………. ……. … ……... .. …………….. …212
- Active Directory Lightweight Directory Services …… ….. .. …. ……………….229
- Resources ……………………………….. .. ..… ……………..………242

مقسم هذا الكتاب الي فصلين

الأول اسمه

- Course 6425A Configuring and Troubleshooting Windows Server® 2008 Active Directory® Domain Services

والثاني

- Course 6426A Configuring and Troubleshooting Identity and Access Solutions with Windows Server® 2008 Active Directory®

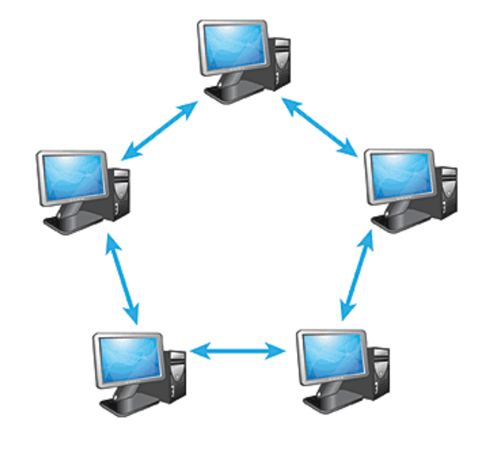
سنتحدث اولا وبإستفاضة عن الفصل الاول

Course 6425A Configuring and Troubleshooting Windows Server® 2008 Active Directory® Domain Services

يتكلم عن اساسيات التعامل مع ال Active Diverter
والتعامل مع المستخدمين والتحكم فيهم

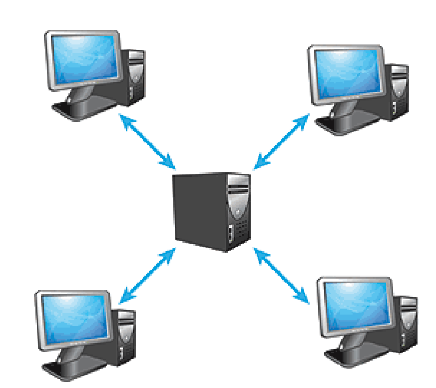
INTRO

قبل البدء في محتويات الكتاب ،، او قبل البدء في مجال الشبكات عموما
يجب علينا ان نفسر بين مصطلحين هاميين جدا وهما :-
Workgroup VS. Domain



- **Workgroup:-**

مجموعه عمل وهي ان كل الاجهزه متصله ببعضها ويستطيع المستخدمين مراقبه او مشاهده او التجسس علي بعضهما البعض
ولا توجد بها اي وسيله من حمايه المعلومات او حمايه خصوصية المستخدمين ولا توجد بها اداره مركزيه
لذا لم يكن من الممكن استخدامها في الشركات الكبيره التي تعتبر الخصوصيه والحمايه من اولوياتها



- **Domain:-**

نظرا للعيوب التي ظهرت من الWorkgroup تم التفكير في الDomain فهو يضمن مركزيه الاداره والمراقبه وحمايه البيانات وكل مستخدم له خصوصياته
ويصعب فيه عمليات التجسس علي الاخرين
كل الاجهزه تكون متصله بالDomain وتسمي Join Domain
ومن خلاله يتم التعامل مع الاجهزه ومراقبتها ومراقبه الشبكه
فهو يتضمن Security and Centralize Administration

إحدي الشركات التي تقدم حلول ال Domain هما ميكروسوفت ولينوكس

- ميكروسوفت عن طريق Windows Server Family .
- لينوكس عن طريق نظم تشغيل متعدده كـRedHat .

في هذا الكتاب سنتكلم عن طريق التعامل مع نظام تشغيل Windows Server المقدم من ميكروسوفت

Windows Server Family
بداية من Windows Server NT وحتي Windows Server 2008 R2
وحاليا كشفت ميكروسوفت عن اصدارها الجديد وهو Windows Server 2012

هناك عدة كورسات لكي تصبح محترفا في Windows Server وهذا الكتاب يتكلم عن أول مادة فيهما وهي
Configuring and Troubleshooting Active Directory

Preparing to Install Active Directory

<u>بعد إجراء عملية تنصيب لوندوز سيرفر ٢٠٠٨</u>

وهذه هي للMinimum requirements لتنصيب Windows server 2008

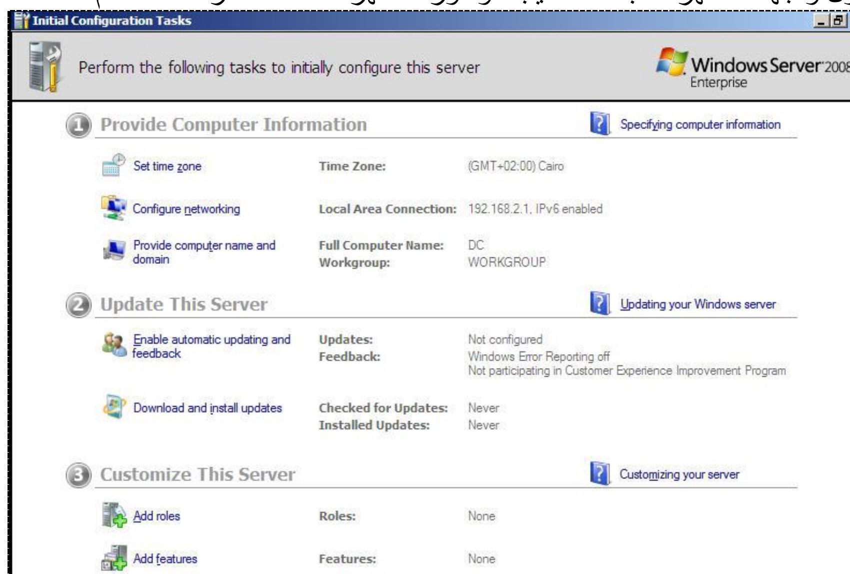
Windows Server 2008 System Requirements

This software is intended for evaluation and deployment planning purposes only. If you plan to install the software on your primary computer, it is recommended that you back up your existing data prior to installation.

To use Windows Server 2008, you need*:

Component	Requirement
Processor	• Minimum: 1 GHz (x86 processor) or 1.4 GHz (x64 processor) • Recommended: 2 GHz or faster **Note:** An Intel Itanium 2 processor is required for Windows Server 2008 for Itanium-Based Systems.
Memory	• Minimum: 512 MB RAM • Recommended: 2 GB RAM or greater • Maximum (32-bit systems): 4 GB (Standard) or 64 GB (Enterprise and Datacenter) • Maximum (64-bit systems): 32 GB (Standard) or 1 TB (Enterprise and Datacenter) or 2 TB (Itanium-Based Systems)
Available Disk Space	• Minimum: 10 GB • Recommended: 40 GB or greater **Note:** Computers with more than 16 GB of RAM will require more disk space for paging, hibernation, and dump files.
Drive	DVD-ROM drive
Display and Peripherals	• Super VGA (800 x 600) or higher-resolution monitor • Keyboard • Microsoft Mouse or compatible pointing device

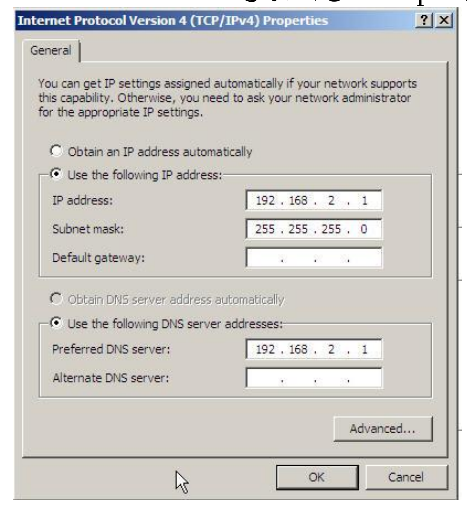
- هذه هي اول واجهه ستظهر لك بعد تصطيب الوندوز ستظهر لك قائمة نادرا ما تستخدم



لكي نظهر ها مره ثانيه:-Start → run → oobe

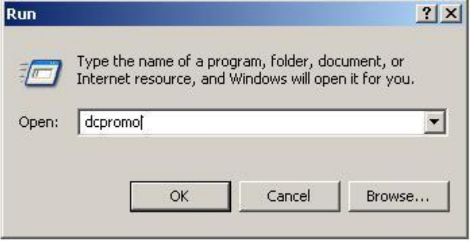
- اولا يجب اعاده تسميه الجهاز بإسم يسهل عليك كتابته بعد ذلك
- ثانيا يجب اعطاء ip للجهاز وsubnet mask

- ثالثا Recommended من ميكروسوفت ان يكون الجهاز المسئول عن الActive Directory هو أيضا المسئول عن خدمه الdns ويكون نفس الip الخاص بالجهاز



بعد ما انتهينا من هذه الاعدادات :-

نقوم بتصطيب ال Active Directory عن طريق كتابه dcpromo في الrun

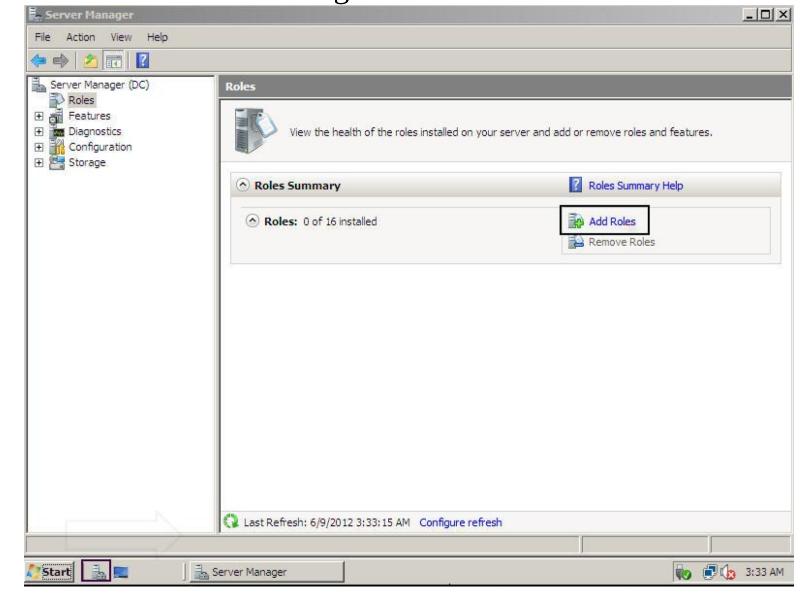


قد تظهر لك Error msg ولن تتم عمليه الdcpromo

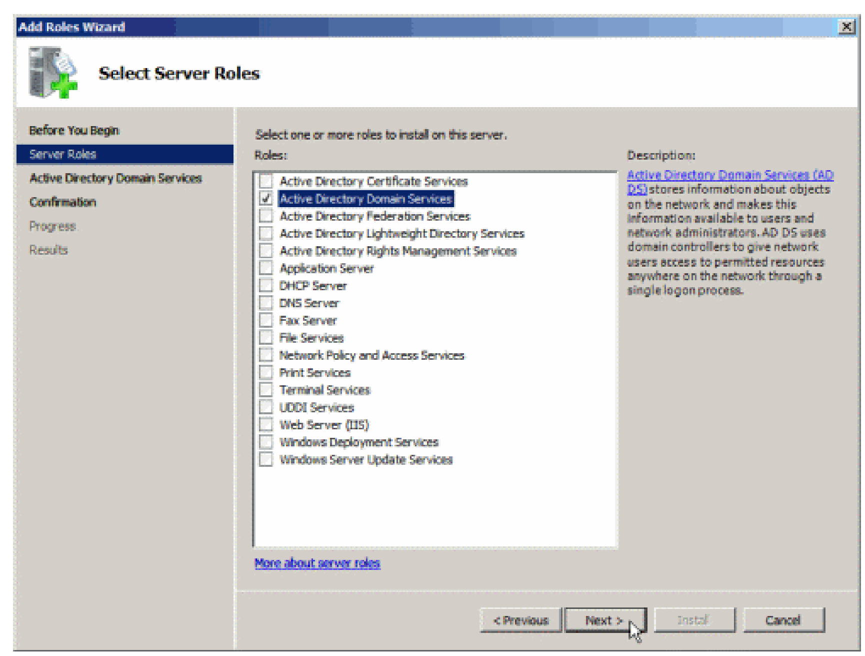


في هذه الحاله نقوم بتصطيب الactive directory domain service binaries

Server manager → Roles → add role



Server role → Active directory domain service



Next →install → Finish

بعد الانتهاء من هذه العمليه سيصبح الجهاز يسمي Domain Controller

بعد ذلك نقوم بإعاده كتابه الامر dcpromo في Run

سنجد انه لا تظهر أي رسائل Errors

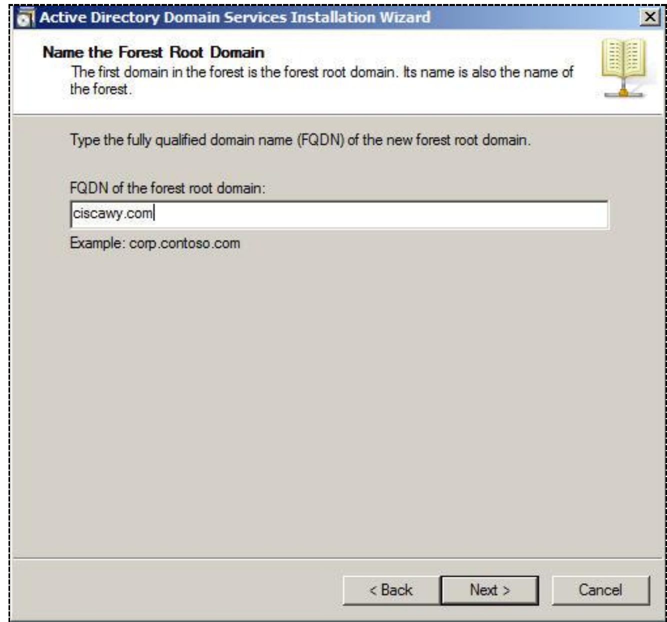


سنستخدم الAdvanced mode لاحقا عند اجراء Child domain

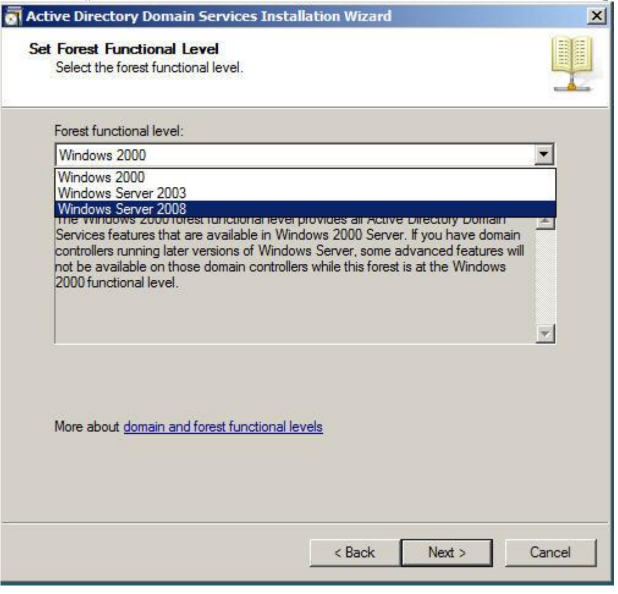


هنختار اننا نعمل Domain جديد في فوريست جديده

سيتم التفرقه بين كل من Forest, Tree, Domain, Child لاحقا



يتم اختيار الFQDN بعنايه حيث انه اما سيكون اسم شركتك او مؤسستك
وممكن بعد ذلك يكون موقعك الرسمي لذا تأني وانت تختاره
بعد ذلك سيتم عمل check سريع للتأكد من عدم وجود اسم شبيه لهذا الDomain في ال Forest الخاصه بك



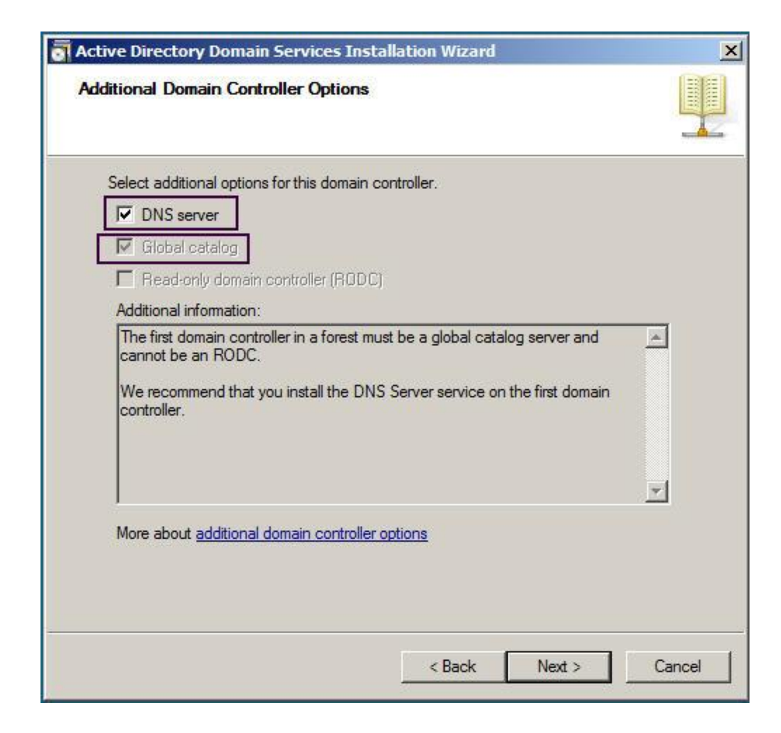
- الForest Function Level

يتم اختيارها علي اساس اخر تحديث للويندوز
حيث انه في سيرفر ٢٠٠٣ كان هناك ٢٠٠٠ و ٢٠٠٣ فقط
وهنا اذا اخترت ٢٠٠٠ او ٢٠٠٣ سيكون باستطاعتك الترقيه الي ٢٠٠٨ ولكن لا يسمح لك بالرجوع من ٢٠٠٨

Forest functional level

Provides a means of enabling additional forest-wide Active Directory features, remove outdated backward compatibility in an environment, and improve Active Directory performance and security.

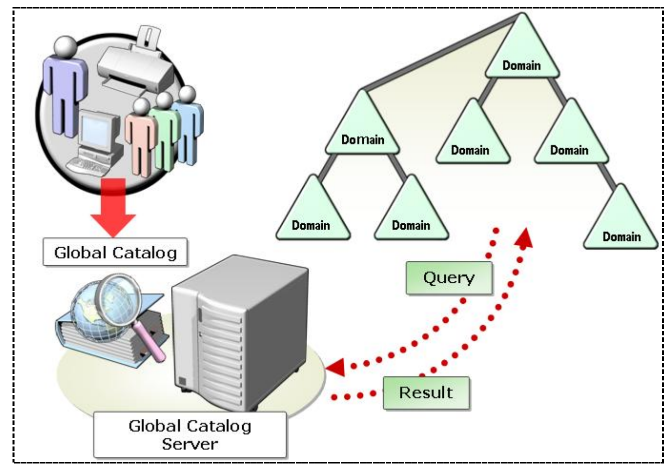
وهامه جدا عند اجراء عمليه ال upgrade من ٢٠٠٣ الي ٢٠٠٨ لأنه يتم فيها raise كل من الDomain والفورسيت الي ٢٠٠٨



كما نوهت من قبل علي موضوع الdns انه كشرط اساسي –ولكنه اختياري- ان يتم تصطيبه علي الMachine التي تلعب دور الDomain Controller
يمكن ان يتم نصطيبه منفردا علي Machine خاصه به وفي اعدادات الIP ندخل الIP الخاص بالDNS

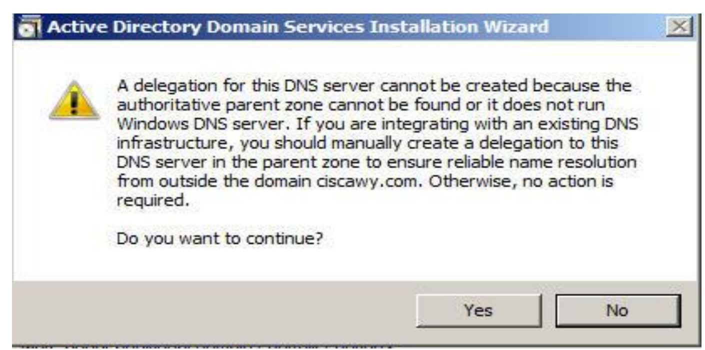
- ولكن ماذا عن الGlobal Catalog (GC) ؟؟

يحتوي ال(GC) علي بعض ال Attributes لكل ال Objects اللى فى كل ال Domains اللى فى الفورست و Any trusted domains

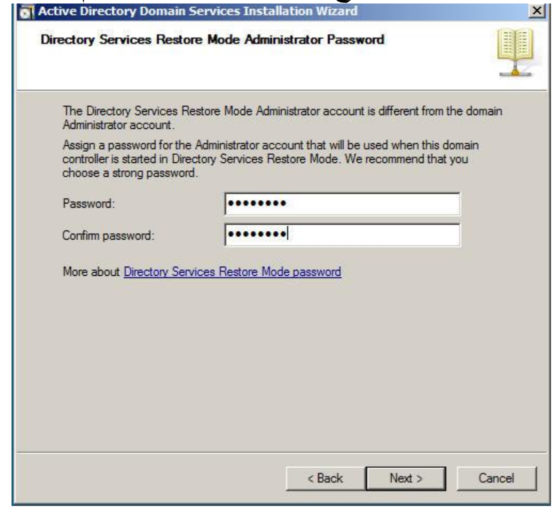


- A partition of the data store called the global catalog (also known as The partial attribute set) contains information about every object in the directory.
- Can be used to locate objects in the directory. Programmatic interfaces such as Active Directory Services Interface (ADSI) and protocols such as LDAP can be used to read and manipulate the data store

اول Domain في الفوريست الخاصه بك يجب ان يكون (GC) By-default لذلك هنا في الصوره ليس اختياريا اما عند تصطيب اي Domain اخر ستجد انها اختياريا
يسرع عمليه الSearch في الDomain بل في الForest ككل



هنختار yes وبعد كدا هتظهر شاشه مكان التصطيب بتاع الdns والad و هنتركهم by-default



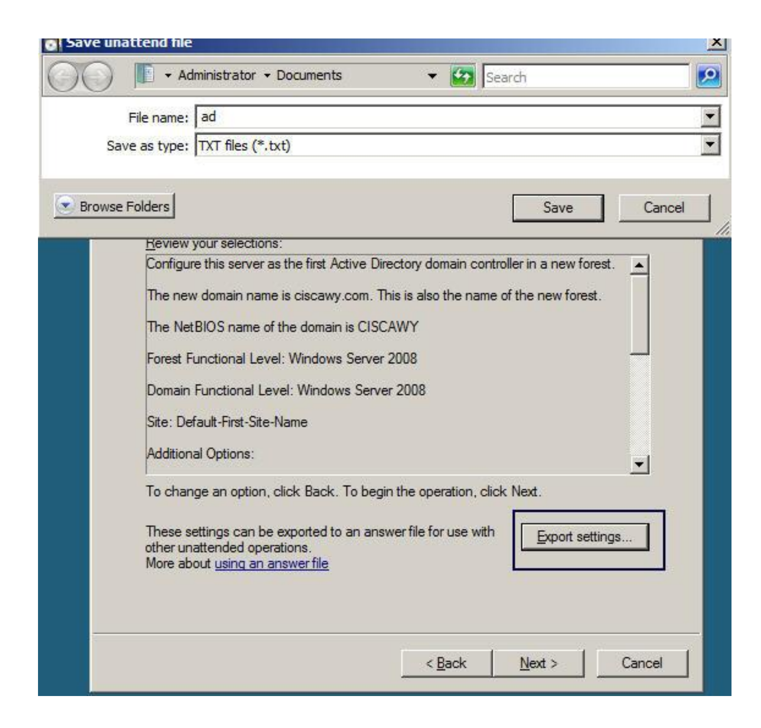
تستخدم كلمه السر هذة في حالة خاصة وهي الRestore mode لإرجاع النسخه المؤخوذ منها الBackp في حاله اذا حدث مشكله في الDomain الخاص بك

لذا تأكد من حفظها جيدا وكتبتها بشكل معقد

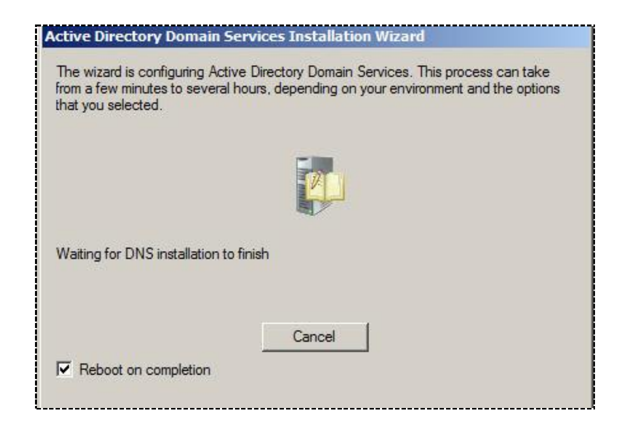
لأنها اذا كانت بسيطه ولا تتوافق مع الRequirements الخاصة بكلمه المرور

ستظهر لك هذه الرساله :-





في حاله اذا اردت الاحتفاظ بالإعدادات الخاصه بالDomain



بعد اعاده فتح الجهاز ستجد الlogin name مختلف

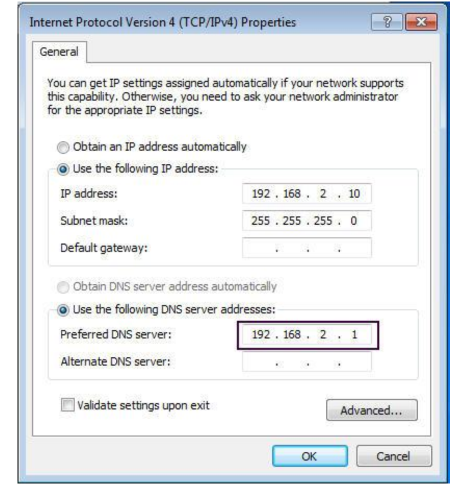


Haw to join a physical computer to domain?

لنأخذ مثال علي هذا جهاز عليه نظام تشغيل وندوز 7

حيث انه يمكن لأي نظام تشغيل وندوز مثل الـXP او الVista ان يرتبط بـDomain Server 2008

- يجب اعطاء الجهاز IP من نفس الRange الموجود علي الDomain Controller
- ويجب ايضا ان يكون له نفس IP الDNS الخاص بال Domain Controller



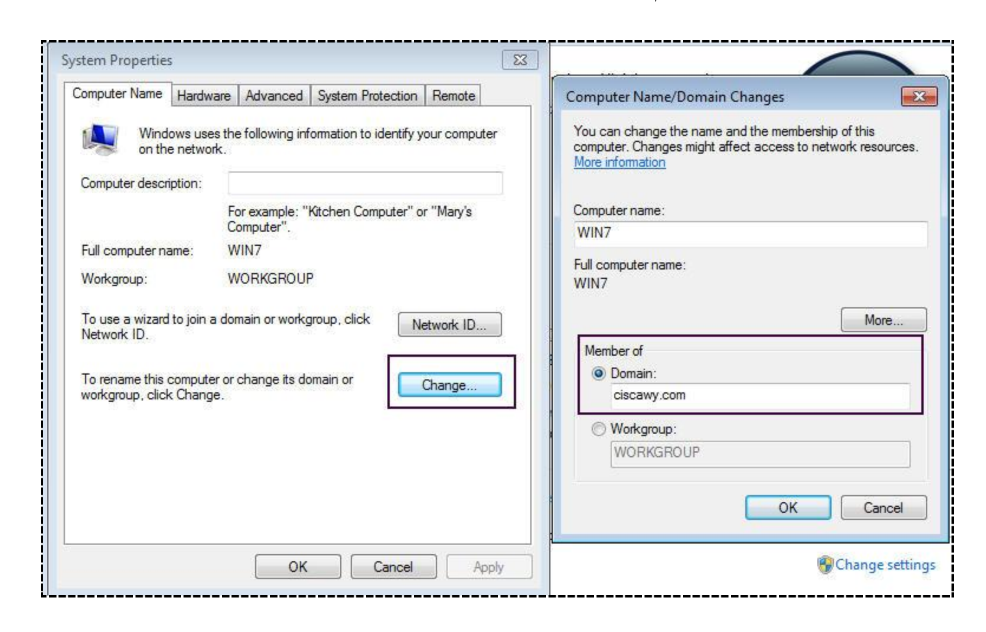
بعد ذلك R.click on my computer → properties

Apple support
Website: Online support
Computer name, domain, and workgroup settings
Computer name: WIN7
Full computer name: WIN7
Computer description:
Workgroup: WORKGROUP
Change settings

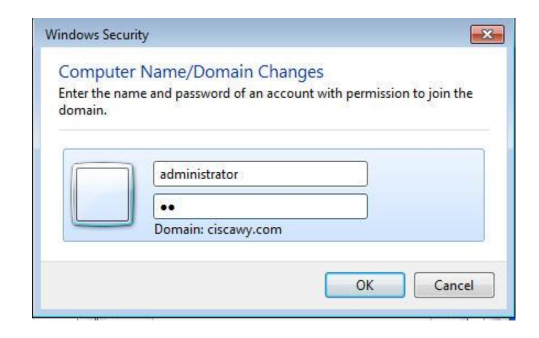
سنجد ان الجهاز Workgroup ← نضغط علي Change setting

ثم نختار Change

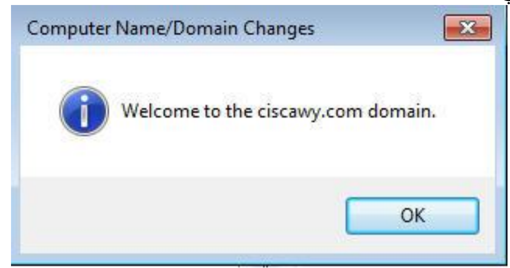
وفي الخانه المخصصه للDomain نكتب اسم الDomain الخاص بنا



ستظهر لنا رساله تطلب منا ادخال الاسم وكلمه المرور الخاصه بالAdministrator



بعد ذلك ستظهر رساله ترحيبيه بنا في الDomain



ثم سيقوم الجهاز بإجراء عمليه Restart مره اخري

Types of AD DS Objects

كل Object له Attribute التي تميزه

User accounts

- Enables a single sign-on for a user
- Provides access to resources

Computer accounts

- Enables authentication and auditing of computer access to resources

InetOrgPerson

- Similar to a user account
- Used for compatibility with other directory services

Organizational Unit

- Used to group similar objects for administration
- Applying group policies

Group accounts

- Helps simplify administration and applying permissions

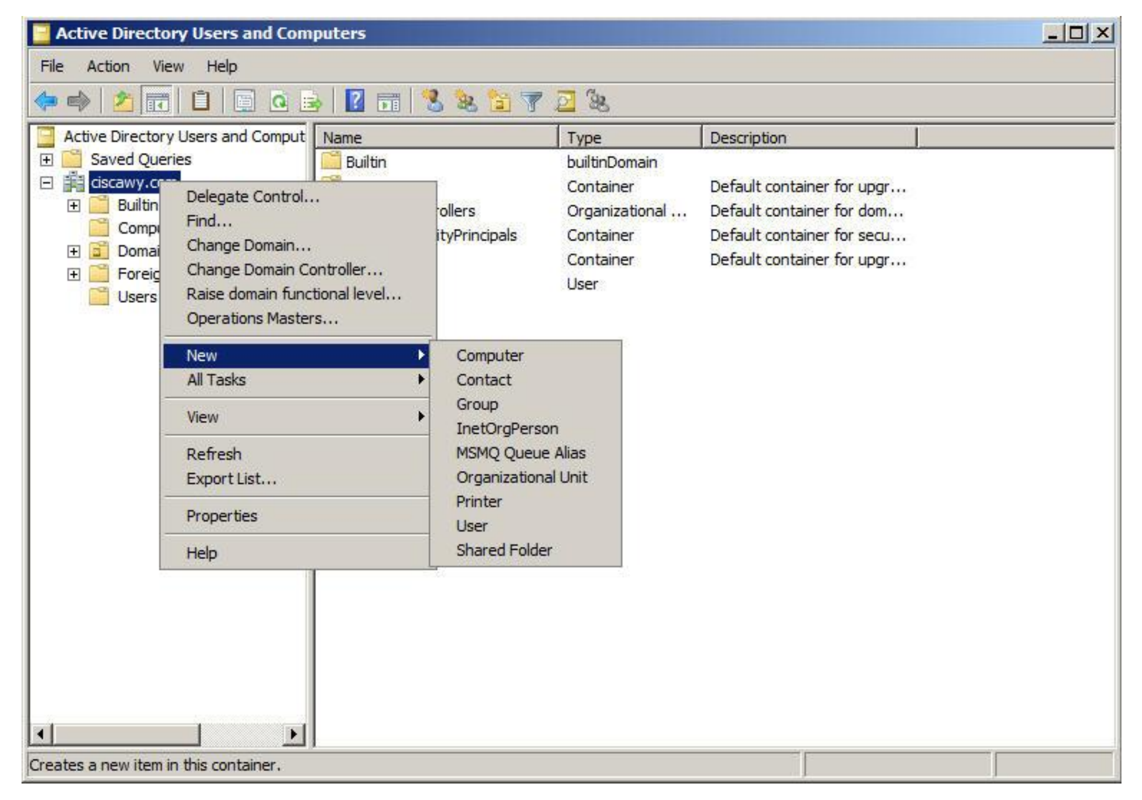
Printers

- Used to simplify the process of locating and connecting to printers

Shared folders

- Used to simplify the process of locating and connecting to shared folders

Start → administrative tools → active directory user and computer
R.click on domain → new

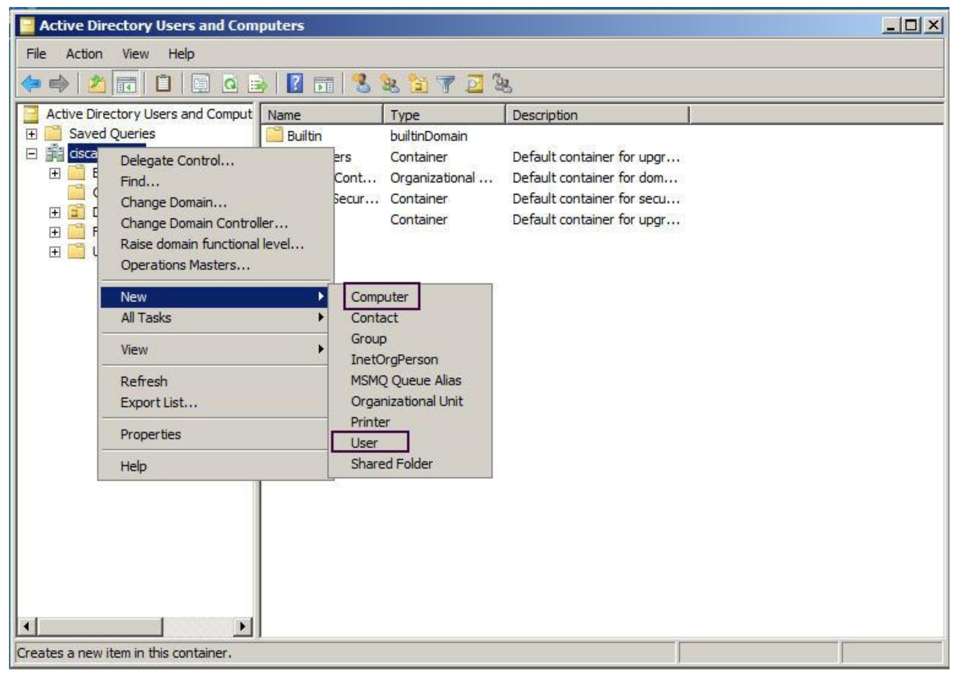


Different between computer and user Account!!

الفرق الجوهري بينهما الاثنين هو ان الـ :-
User Account معنوي يعني ليس ملموس في الحقيقه وليس شرطا ان يكون عدد الUsers مساو لعدد Computers بل بالعكس يفوق عددهم
لأنه ليس شرطا ان يكون لكل User → Computer ولكن شرطا ان يكون لكل Computer → User "مستخدم"
Computer account مادي ملموس و هو اقل في العدد عن User Account

How to create each of them?

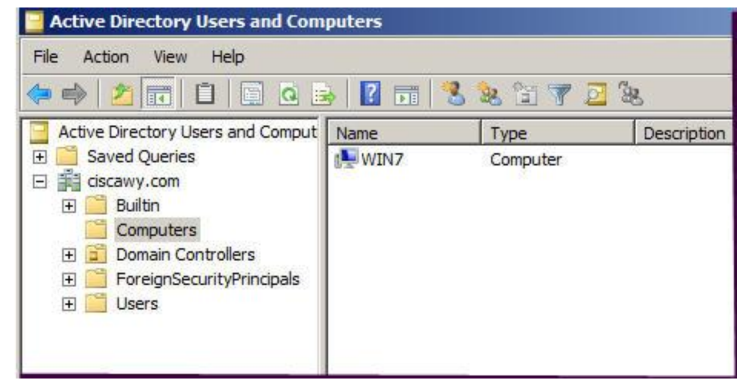
Start → administrative tools → active directory user and computer
R.click on domain → new



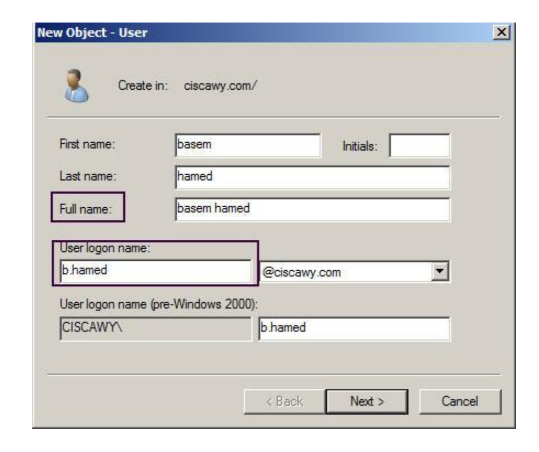
Computer account

قبل سيرفر 2000
- كان يجب علي مدير الشبكه ان يقوم بانشاء Computer Account لأي جهاز ثم بعد ذلك نقوم بأجراء Join to Domain

اما منذ اصدار سيرفر 2003 وحتي الأن اصبح بمجرد ان يقوم الجهاز بعمل Join يتم انشاء حساب له في الContainer الخاص بال Computer



User Account



عند انشاء User Account
ليس شرطا ان يكون الLogon name هو نفس الFull name
ال Full name هو ما يظهر له في قائمه Start اما اسم الدخول هو ما يقوم بالدخول به الي الجهاز



- يجب ان تكون كلمه المرور معقده كأسلوب حماية من ميكروسوفت

عند انشاء اكثر من User يجب ان تختار اول اختيار وهو ان User يتوجب عليه ان يغير كلمة المرور عند دخوله المره القادمه حتي يكون كل مستخدم مسئول عن كلمه المرور الخاصه به بعيدا عن مدير الشركه

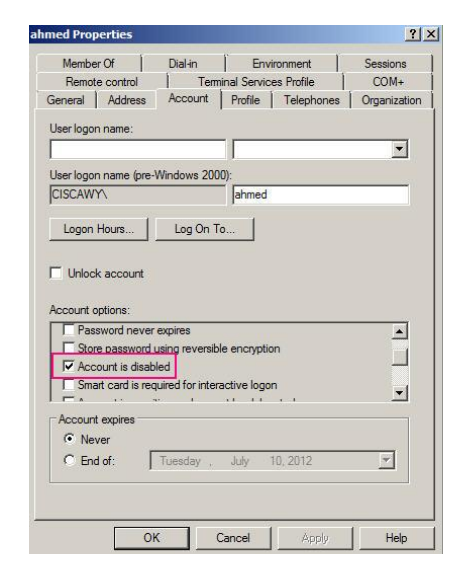
- اما الاختيار الاخير Account Disable

فهو يستخدم عند انشاء حساب لمستخدم قد يتعاقد معه قريبا ،، او اذا كان هذا المستخدم سيعمل خارج الشركه لفترات كثيره ففي هذه الحاله يكون حسابه غير متاح لحين عودته
حتي لا يستطيع اي احد من الHackers استخدام هذا الحساب والتجسس الي شركتي خصوصا لو كان صاحب هذا الحساب له مركز حساس في الشركه

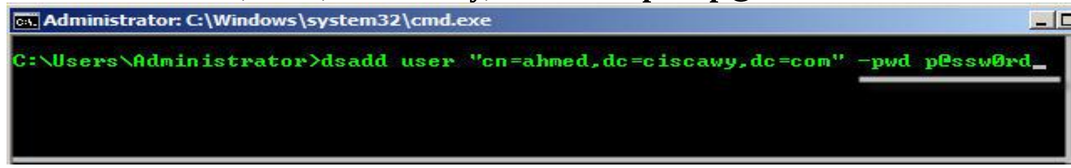
ولكن هل يتوجب علي حينما اقوم بإنشاء اكثر من 100 User Account ان اقوم بهذه الخطوات !!
بالطبع لا ،،،،
هناك امر يكتب في الcmd → run يمكن من خلاله انشاء عدد لا نهائي من الusers

dsadd user "cn=ahmed,ou=it,dc=ciscawy,dc=com"
dsadd → domain services
cn → canonical name

معني الامر انشأ يوزر اسمه ahmed في الou اسمها it علي الDomain اللي اسمه Ciscawy
ولكن اذا تم اجراء هذا الامر الUser Account سيكون Disabled لأننا لم نقم بإعطاءه كلمه مرور ولذلك تعتبر كلمه المرور شئ اساسي جدا حينا نقوم بإنشاء الUser Account عن طريق الcmd



dsadd user "cn=ahmed,ou=it,dc=ciscawy,dc=com" –pwd p@ssword



dsadd ou "ou=sales,dc=ciscawy,dc=com"

انا عايز انشأ ou اسمها sales للDomain اللي اسمه Ciscawy

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>dsadd user "cn=ahmed,ou=it,dc=ciscawy,dc=com"
dsadd succeeded:cn=ahmed,ou=it,dc=ciscawy,dc=com

C:\Users\Administrator>dsadd ou "ou=sales,dc=ciscawy,dc=com"
dsadd succeeded:ou=sales,dc=ciscawy,dc=com

C:\Users\Administrator>_
```

DS commands :-

The following DS commands are
Supported in Windows **Server 2008 R2:**

- DSadd → Creates an object in the directory.
- DSget → Returns specified attributes of an object.
- DSmod → Modifies specified attributes of an object.
- DSmove → Moves an object to a new container or OU.
- DSrm → Removes an object, all objects in the subtree beneath a container object, or both.
- DSQuery → Performs a query based on parameters provided at the command line and returns a list of matching objects

- وبكدا ممكن اعدل في الامرعلي حسب الغرض اللي أريده سواءUser او Group او OU وانسخه اكثر من مره واعمله paste في ال cmd وكلهم هيتعملهم create لعددهم مره واحده في المكان اللي انا محدده

- تسهيلا لعميلة البحث عما يمكن اضافته بإستخدام امر **dsadd** :-

يمكنك الاستعانه بالHelp and Support الموجود في Windows Server وكتابه dsadd في خانه البحث وستظهر لك كل النتائج المتعلقه بهذه الكلمه

- -: User Templates

ممكن ان نقوم بإجراء كل الخصائص Attribute التي نريدها في كل ال Users المخولين بإجراء شئ محدد علي الDomain

و هي ان نقوم بتعديل كل هذه الخصائص علي User معين ثم نقوم بـ copy → R.click on user

وسنقوم فقط بتغيير الاسم وكلمه المرور ولكن كل الAttribute ستكون موجوده

- -: Security Identifier

هو عبارة عن رقم تعريفي خاص بأنظمة مايكروسوفت ويعادله في أنظمة لينوكس UID ويتم إنشائه بشكل تلقائي لأي حساب جديد على السيرفر (الشبكة) أو جهاز الكمبيوتر الخاص، حيث أن هذا الرقم مخلتف من حساب لآخر أي أنه فريد من نوعه Unique،

ويخزن فيه جميع الميزات والتصاريح المخولة لذلك الحساب.

حيث انه عندما نقوم بنقل الUser من Domain لأخر حتي و ان كان بنفس الاسم لا تحدث مشكلة نظرا لوجود الSID

و هو عادة يكون على الشكل التالي S-1-5-32-1045337234-12924708993-5683276719-19000 :

لمعرفه الSID الخاصة بك

Run → cmd → whoami/user-:

Types of Users

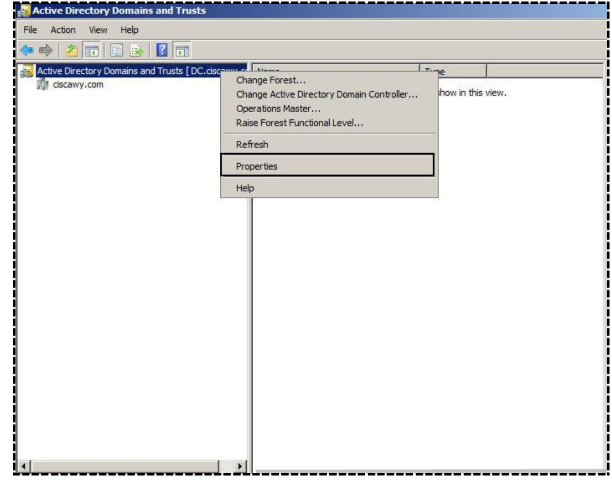
- Power user → Under Administrator Account
- Guest user → By-default Disabled
- Limited user → Do What Created For يفعل ما انشأ له

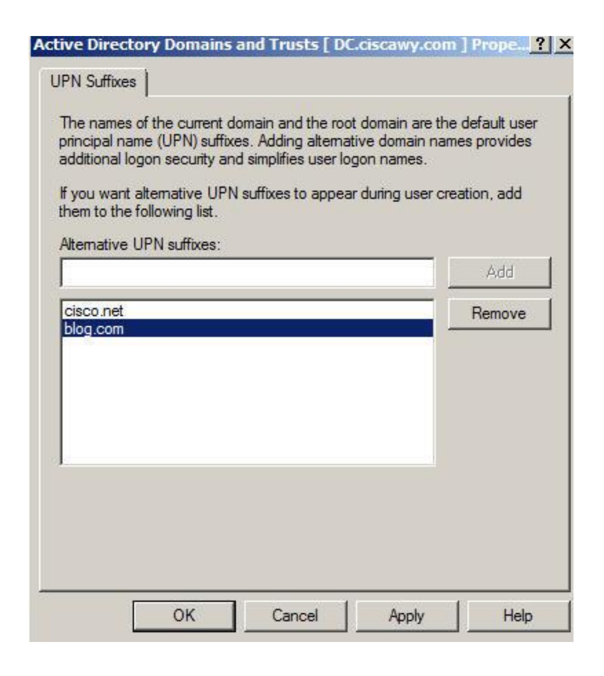
UPN → User Principal Name

تستخدم هذه الخاصيه حينما اريد ان اضيف اكثر من اسم لنفس ال Domain الخاص بي

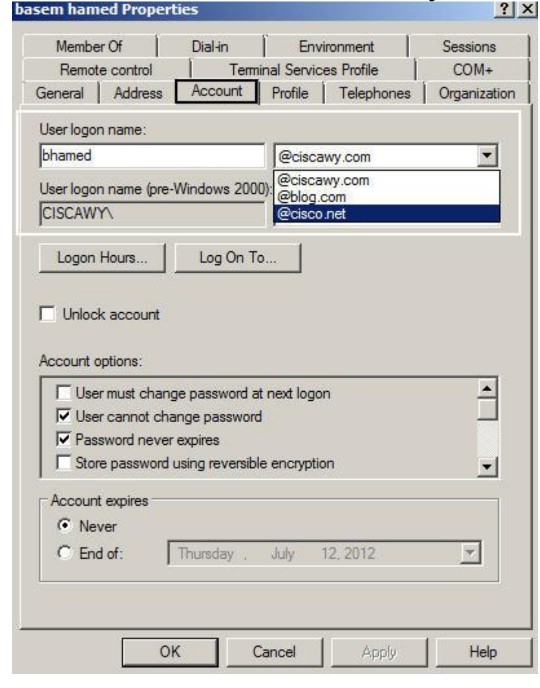
ويتم تعديل في الLogon الخاص بالUser سواء كان بإسم الDomain الرئيسي او بالاسم البديل

Start → administrative tools → active directory domains and trust





Start → administrative tools → active directory users and computers



بحدد من هنا عايز الUser يدخل بانهي اسم Domain

علي الجهاز الخاص بوندوز 7 هندخل الupn الخاص باليوزر بعد تعديل ال@



Computer name, domain, and workgroup settings

Computer name:	WIN7	Change settings
Full computer name:	WIN7.ciscawy.com	
Computer description:		
Domain:	ciscawy.com	

سنجد ان اسم الDomain لم يتغيير بل تغير فقط اسم الدخول
وهذه الخاصيه تعتبر كـ Security Wise من ميكروسوفت في ان يكون اسم الDomain الرئيسي مخفي عن أعين المخترقين بالـ Foot Printing تتبع الاثار،، لمعرفه الاسم الحقيقي لDomain الخاص بي وبالتالي يتم اختراقه بل الافضل التعامل بأسم بديل

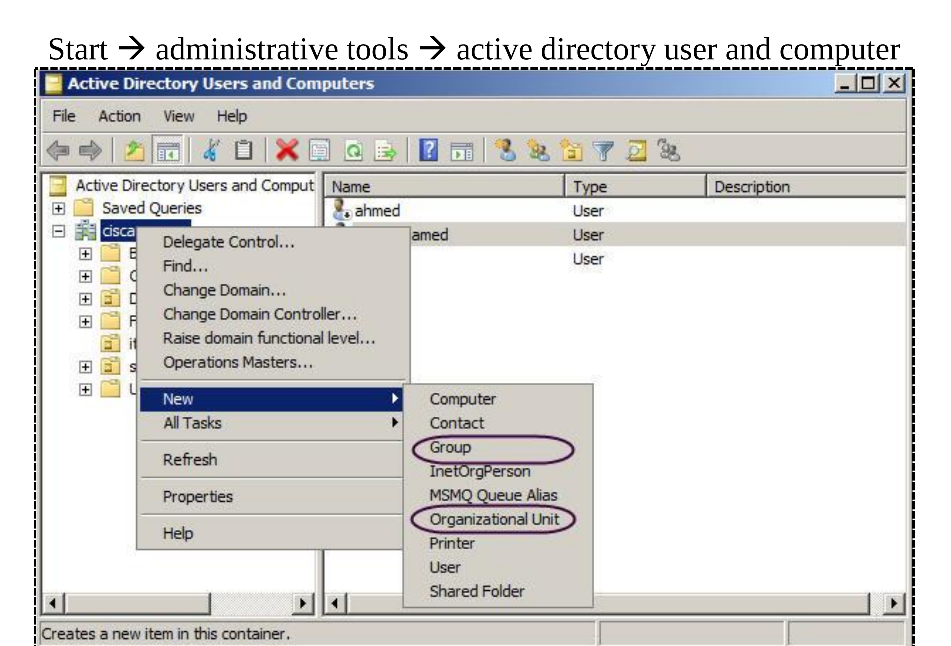
حتي تأمن اكبر قدر من الحماية لخصوصيات الDomain الخاص بك

Groups VS Organization unit

كلاهما يقوم بوظيفه معينه وهي تطبيق Restrictions علي المستخدمين
سواء كانت صلاحيات Permissions او سياسات Policies

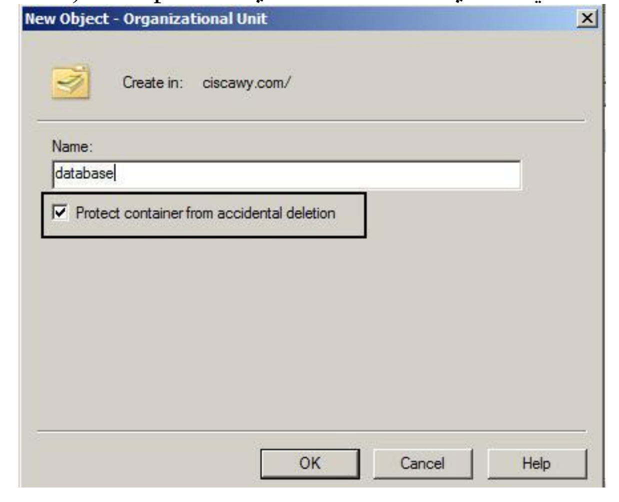
ولكن الإختلاف بينهما :-
Groups: - تطبق علي المستخدمين بعض الصلاحيات علي الملفات مثل read, write...
عن طريق ال Shared folders
O.U :- تستخدم لتطبيق القيود علي المستخدمين والحد من حريتهم علي الاجهزة
عن طريق الGroup policy

Start → administrative tools → active directory user and computer



Ou . Organization unit

- تستخدم كأداه تنظيميه للDomain الخاص بي
- الغرض منها تنظيم العمل والادارة في الActive Directory
- يجب ان تختار اسم الوحده التنظيميه OU علي حسب الغرض الذي انشأت من اجله حتي تسهل عليك عمليه ال Monitor & Troubleshoot اذا حدث اي مشاكل في الDomain
- او تسميها علي حسب مهام من بها من المستخدمين
- يطبق عليها الGroup policy سواء علي مستوي الUser او مستوي الComputer (سنتحدث عنها لاحقا)

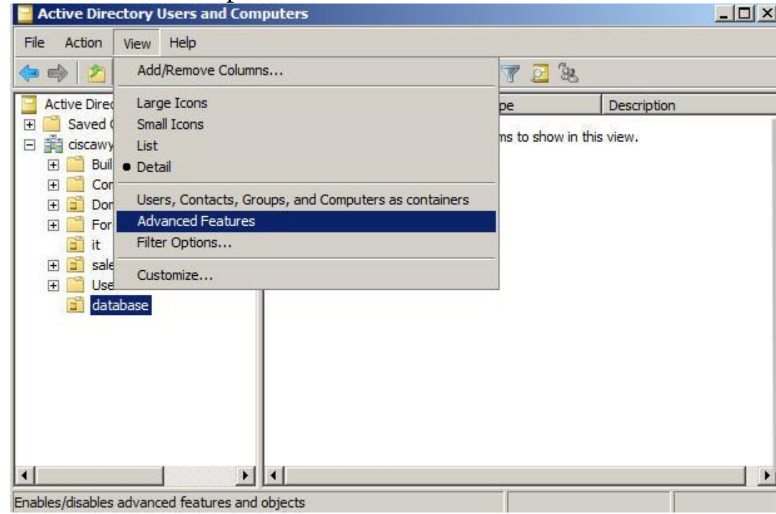


حينما تقوم بإنشاء وحده تنظيميه جديده ستجد Protect Container from Accidental Deletion موضوع بها علامه صح . ✓

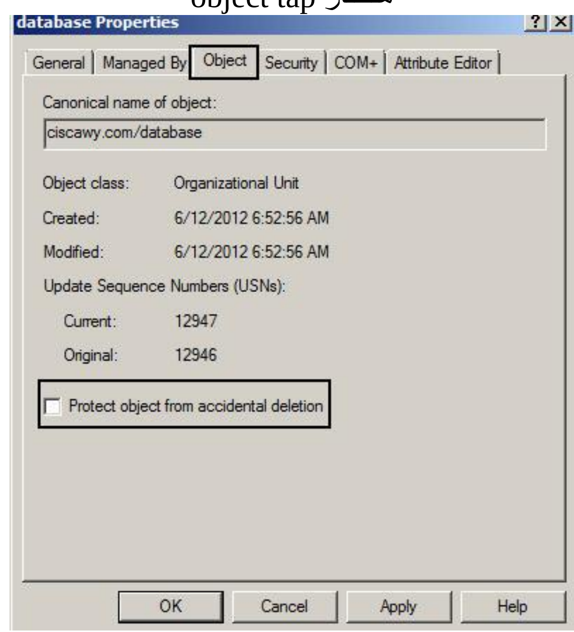
ومعناها ان تكون هذه الوحده التنظيميه OU لا يستطيع اي احد ان يقوم بحذفها فهي Protected
و هذا لأن OU يكون شأنها هام جدا من حيث تنظيم الDomain لذلك يجب ان يكون لها حماية خاصة
جرب بعد الانتهاء من انشائها ان تحدفها ،، ستجد انك لا تستطيع !!

فأذا اردت ان تحذفها :-

Tap View → Advanced feature



R.click on OU that you want to delete → properties
هتختار object tap



ونحذف الprotect ثم بعد ذلك سيسهل حذفها ..

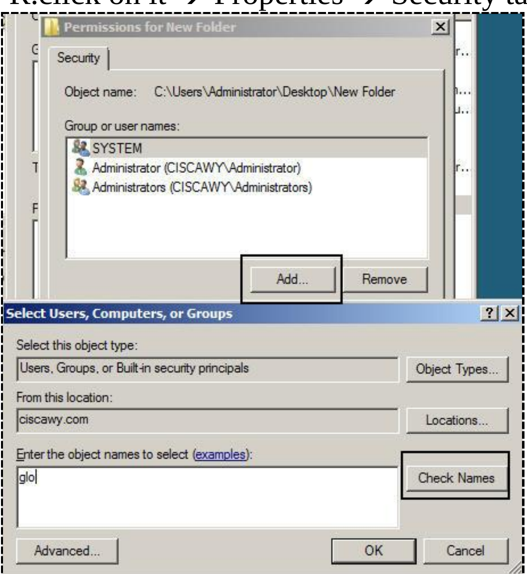
GROUPS

الغرض منها تطبيق صلاحيات Permissions لمجموعه من المستخدمين علي ملف معين
Read, write, full control

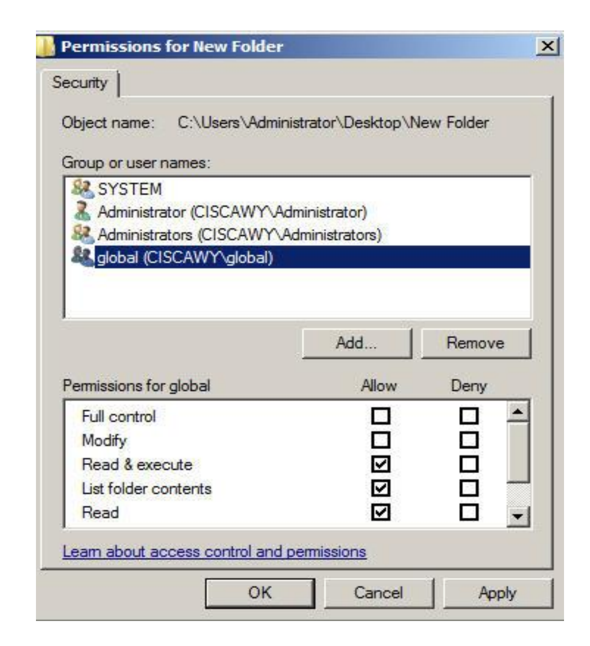
Start → administrative tools → active directory user and computer → R.click → new Group



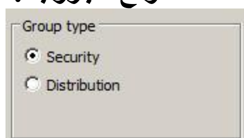
بعد انشاء الجروب نضع بها كل المستخدمين الذين نريد ان نطبق عليهم صلاحيات permissions معينه
ثم نقوم بإنشاء فولدر Edit → Security tap → Properties → R.click on it



نضغط علي Add ثم نكتب اسم الGroup ونضغط علي Check name يتظهر لنا الجروب
ثم نختار الصلاحيات المخوله لها
واذا كان الUser له صلاحيات والGroup لها صلاحيات اخري ،، فإن الاكثر تعقيدا هي التي ستطبق علي الUser
Most Restrictive
(Deny over write allow)



- **انواع الجروب :-**



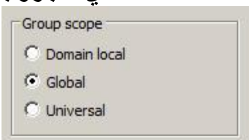
❖ Distribution group

◊ مجموعه للتوزيع
◊ تستخدم في ارسال الemail – اذا كان لديك mail server او exchange فحتما ستستخدم جروب للتوزيع حيث انها اسرع ولا تحتاج الي عمليات وثوقيه من الDomain للإرسال والاستقبال
◊ علي عكس ال security group

❖ Security group

◊ مجموعه للحمايه
◊ تستخدم لإضافه بعض الpolicy و الroles علي المستخدمين
◊ يمكن ان تستخدم في ارسال الemail ولكنها ستكون بطيئه للغايه حيث انها ستحتاج الي وثوقيه من الDomain والسماح لها من ان ترسل من مستخدم لأخر
◊ ولكنك اذا رأيت في ارسال الemail داخلي لا يكون هناك delay نهائيا

- **مدي الجروب group scope**

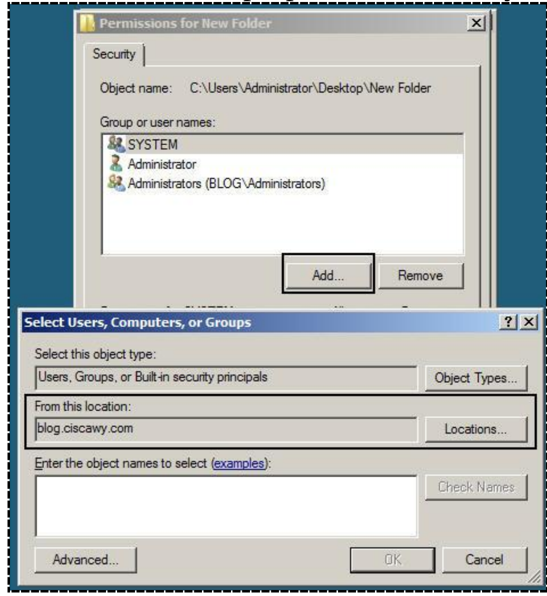


	Members	Access = Permission
▪ **Global Group**	تحتوي علي مستخدمين من نفس الDomain فقط Contain user from the same domain only	اي Domain بينهم ثقه متبادله Member permissions can be assigned in any trusted domain
▪ **Domain Local**	تحتوي علي مستخدمين من اي Domain Contain users from any domain	الصلاحيات من الDomain الداخلي فقط Member permissions can be assigned only within the same domain

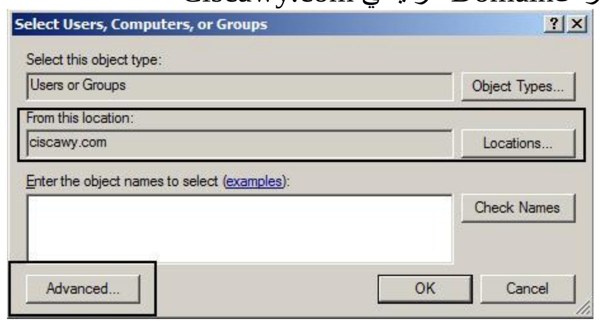
▪ **Universal**	تحتوي علي مستخدمين من اي Domain Contain user from any domain Saved-in Global Catalog	الصلاحيات علي اي Domain Permission on any trusted domain

✓ حاليا قمت بإنشاء"blog.ciscawy.com" child domain (سنتحدث عنه لاحقا) لغرض ان نفهه هذه الجزئيه
✓ قمت علي الDomain الرئيسي بإنشاء 3 groups بانواعها
✓ نقوم علي الchild domain بإنشاء shared folder

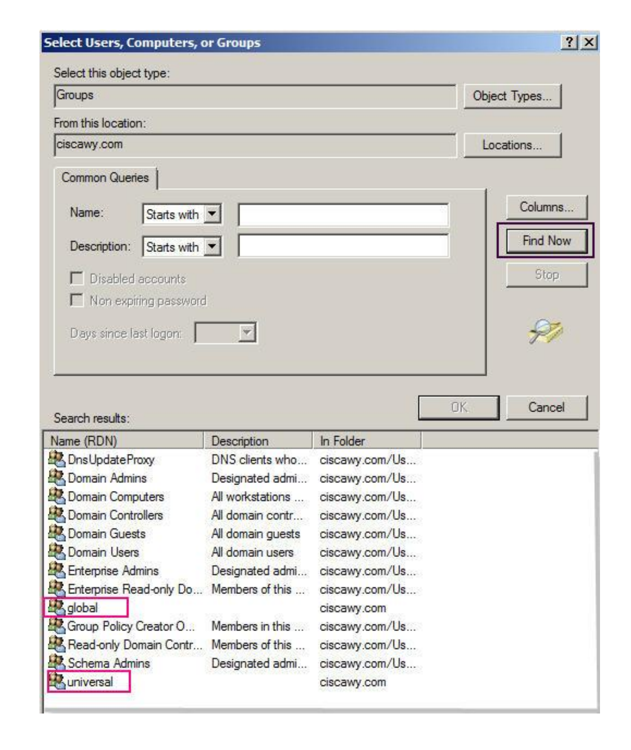
R.click on shared folder → properties → security tap → Edit



نقوم بتغيير الLocation ونختار الDomain الرئيسي Ciscawy.com



ثم نضغط علي advanced لنقوم بعمل بحث علي كل ال object الموجوده



سنجد فقط الglobal والuniversal ولن تجد الdomain local حيث ال domain local

Domain Local	تحتوي علي مستخدمين من اي Domain Contain users from any domain	الصلاحيات من الDomain الداخلي فقط Member permissions can be assigned only within the same domain

تأخذ صلاحياتها من الDomain الخاص بها فقط !!تحويل من نوع لأخر
Global → **convert to** Universal → **convert to** domain local

- **NESTED التعشيش**

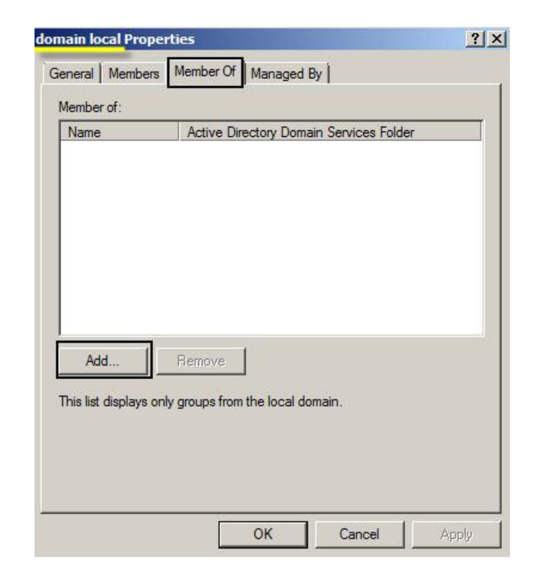
او كمصطلح اخر Being a Member :-

١- **Member of OR Nest of**

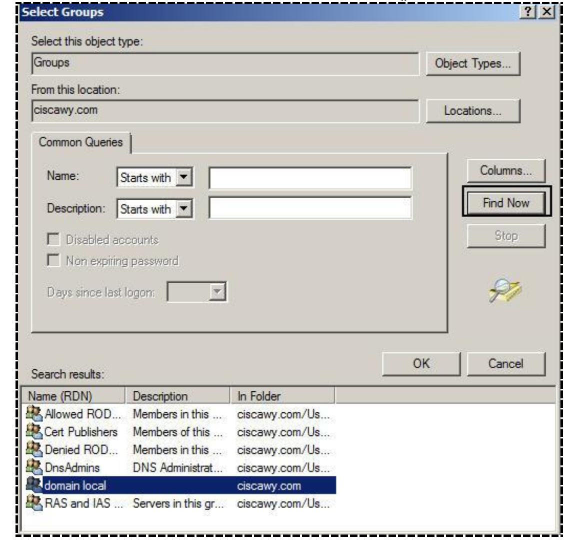
TYPE	MEMBER OF
▪ Global	Universal Domain local Global
▪ Domain Local	Only Domain Local
▪ Universal	Universal Domain Local

Double click on any Group ⇦ونختار Member of ثم Add

نأخذ مثلا ... Domain local



ثم نضغط علي Advanced ثم بعدها Find now
سنجد ان ال Domain local فقط هي التي ستكون موجوده
وبالتجربه من باقي الGroups سنجد كما دونت في الجدول

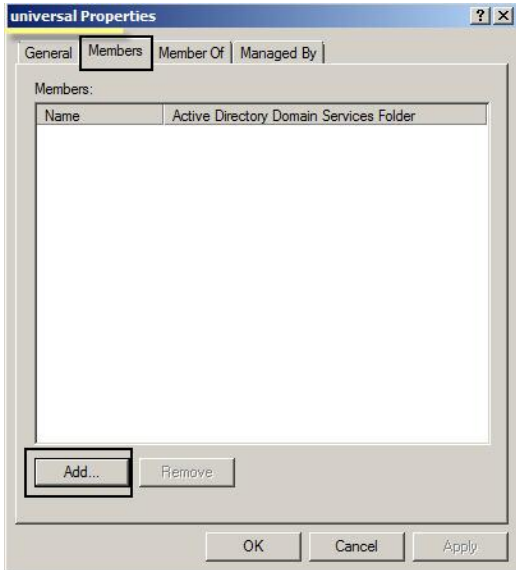


٢- **Member in OR Nest in**

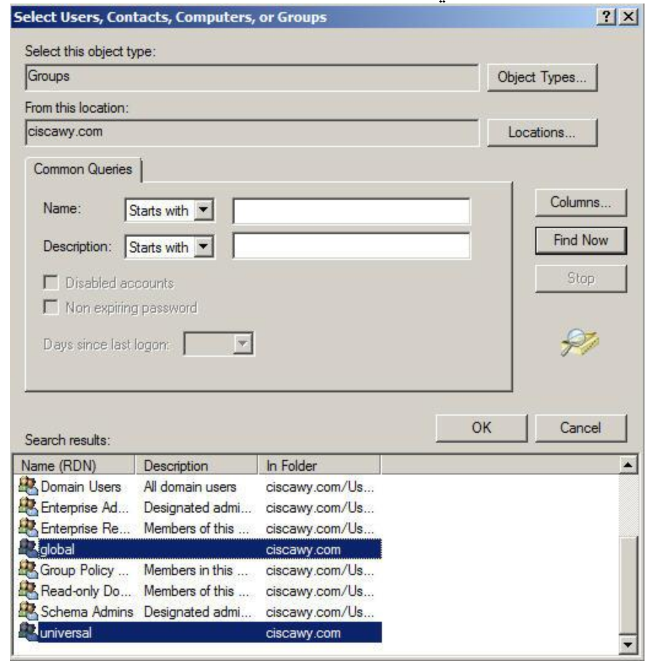
TYPE	MEMBER IN
▪ Global	Global
▪ Domain Local	Universal Domain local Global
▪ Universal	Universal Global

Double click on any Group ⇦ونختار Member of ثم Add

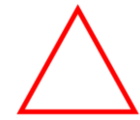
نأخذ مثلا ... Universal



ثم نضغط علي Advanced ثم بعدها Find now
سنجد ان ال Universal و ال Global سيكونوا متواجدين
وبالتجربه من باقي الGroups سنجد كما دونت في الجدول



الفرق بين Forest , Tree , domain



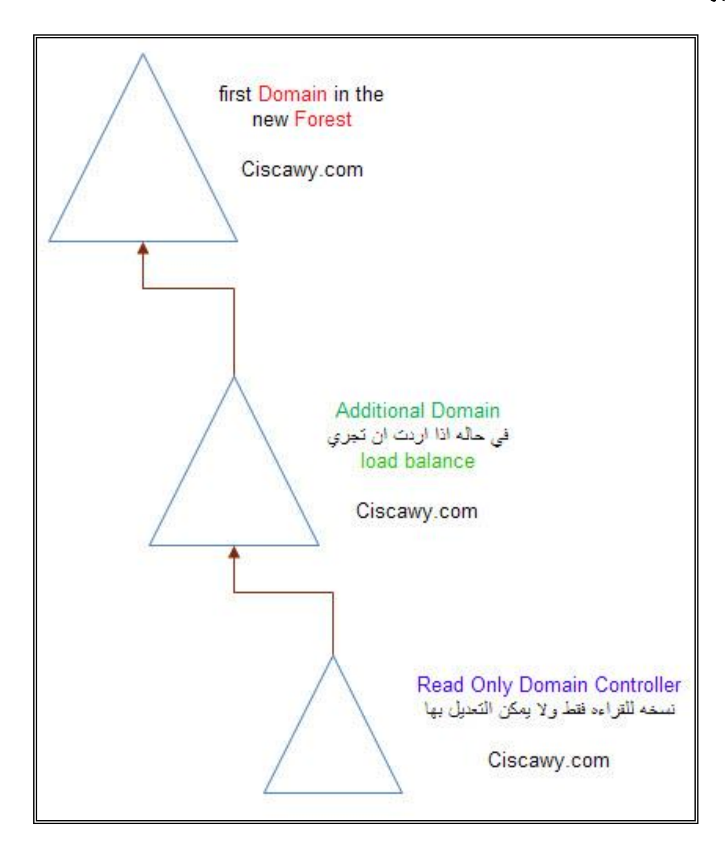
يرمز للDomain كشكل مثلث كتسهيل في عمليه الشروحات او الرسوم التوضيحيه

بعد اجراء أول عمليه تنصيب Windows Server٢٠٠٨ واجراء عمليه الترقيه الي Domain بكتابه dcpromo ينفرد هذه الDomain بعده خصائص :-

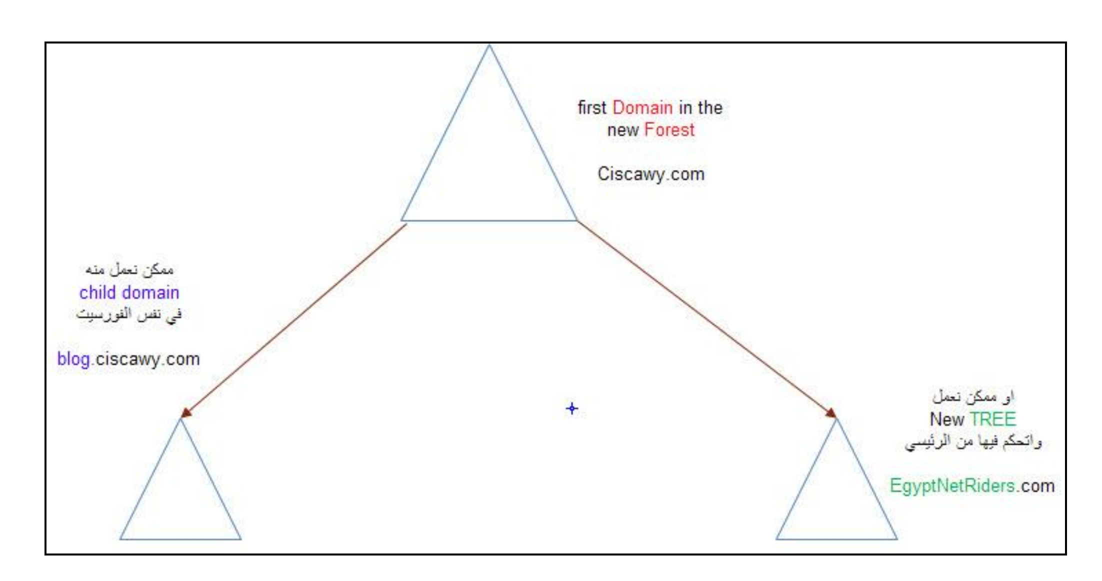
اول Domain في ال Forest الخاصه بي

- وبإختيار اسم الDNS يصبح هذا الاسم هو اسم الForest
- يسمي The Primary Domain أو First Root Domain
- يكون Global Catalog by default
- يصبح default first site name
- في الغالب يجب ان يكون ال DNS Server
- **ممكن من خلاله اقوم بعمل :-**

- Additional domain نفس اسم الDomain الرئيسي ويمكن اجراء تعديلات به ، في حاله اذا كنت اريد اجراء علميه توزيع للحمل Load Balance اذا كان هناك حمل كبير علي الDomain الرئيسي
- Read Only Domain Controller نفس اسم الDomain الرئيسي ولكنها نسخه للقراءه فقط ولا يمكن التعديل بها



- Child domain اذا كنت اريد ان انشأ Domain Sub Domain صغير له خصائصه المستقله واريد التحكم فيه من خلال الDomain الرئيسي عن طريق فقط الEnterprise Administrator
- New Tree اذا حدث تعاقد بين شركتي وشركه اخري واردت ان يكوم مدير الشبكه عندي هو المسئول عن الشركتين ولكني اريد ان يكون مستخدمي الشركه الثانيه يتعاملوا بنفس اسم الDomain الخاص بهم – كما حدث مع شركتي Oracle & Sun – في هذه الحاله انشأ Tree جديده ولكن يكون التحكم من خلال الDomain الرئيسي عن طريق فقط ال Enterprise Administrator



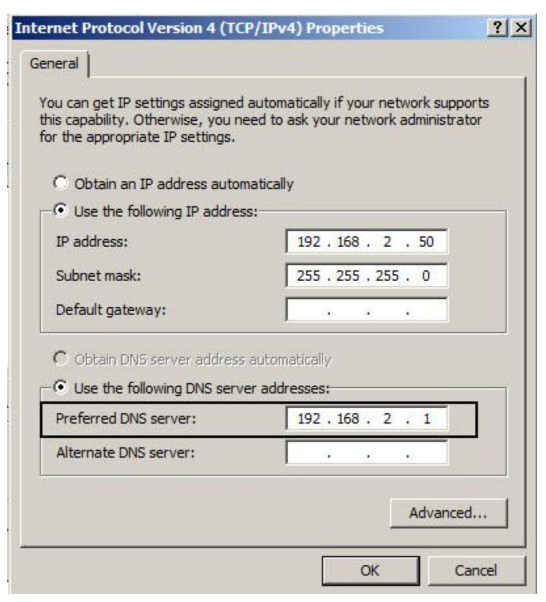
- الDomain هو النطاق الذي اعمل بداخله أين كان نوعه …., Tree , Additional , Child .
- وكل Domain الmachine التي يعمل عليها تسمي Domain Controller
- اما الActive Directory فهو الDatabase قاعده البيانات اللي بتعامل معاها

خلاصه القول
Forest → Many Trees → many Different Domains
Forest → many Different Domains

لنتعرف علي كل منهم بالتفصيل

Additional domain

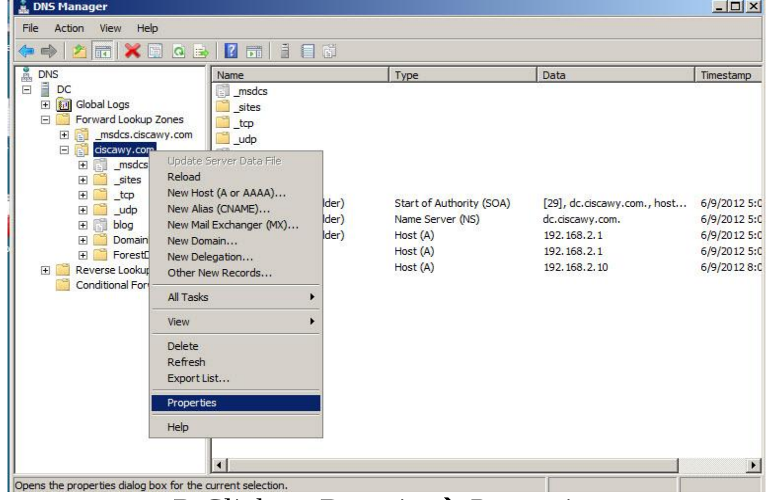
- ✓ نسخه من الDomain الرئيسي
- ✓ لغرض تقليل الحمل علي الDomain الرئيسي اذا زاد عدد ال users عن ٥٠٠ او كنا نملك مؤسسه كبيره
- ✓ أي اقوم بعمل Load Balance بين الDomain الرئيسي وال Additional
- ✓ عندما اقوم بإنشاء اي Object علي احداهما يتم انشاءه في الاخر في نفس الوقت
- ✓ عندما يقوم Users بالاتصال بالDomain يتم الاستجابه بالتناوب
- ✓ ينشأ علي Machine خاصه به ،، وليس علي Machine الDomain الرئيسي
- ✓ اعدادات ال TCP / IP :-



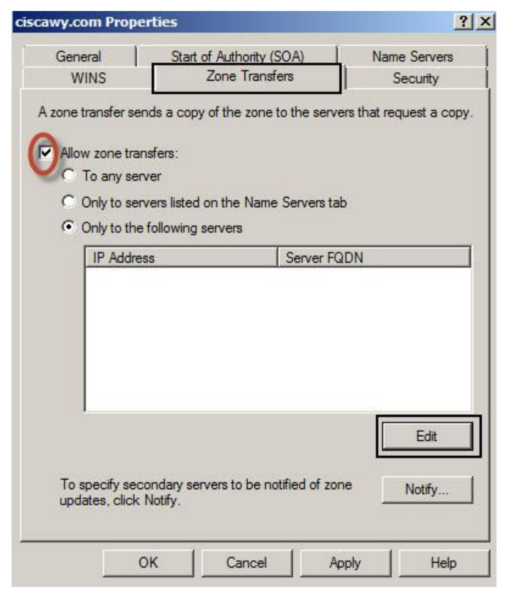
- يجب ان يكون الDNS هو نفس الIP الخاص بالDomain الرئيسي

✓ علي الDomain الرئيسي نقوم بفتح DNS → Start → Administrative tools

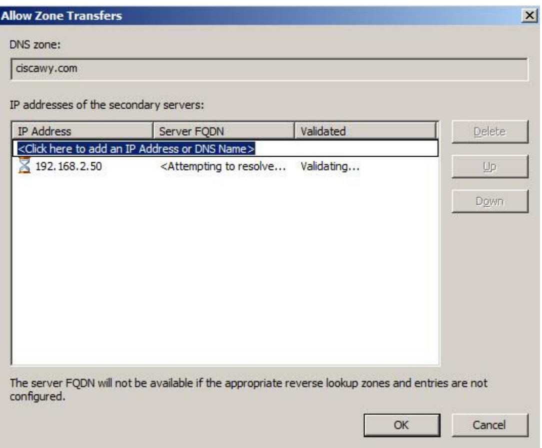
حتي نقوم بإنشاء ما يسمي Zone Transfer وهي من ستكون مسئوله عن عمليه ان كل Domain يقوم بالتداول (بمعني ان كل Domain يجيب بالتناوب مع الاخر)



R.Click on Domain → Properties



Zone Transfer tap → Allow transfer → Only this domain → EDIT نختار



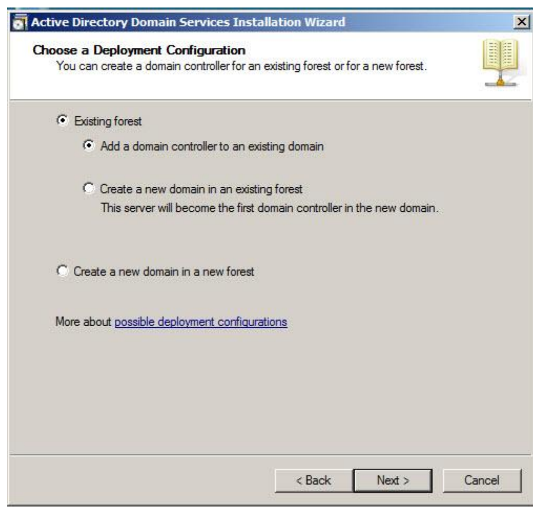
نكتب الIP الخاص بالmachine التي ستلعب دور ال additional domain
Ok → ok

- علي ال Machine الجديده التي ستقوم بدور الAdditional

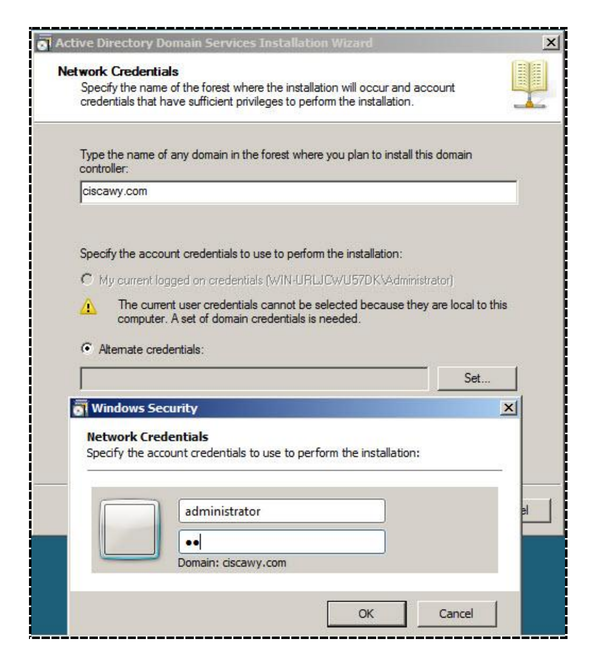
Run → cmd → dcpromo



نضغط علي Next

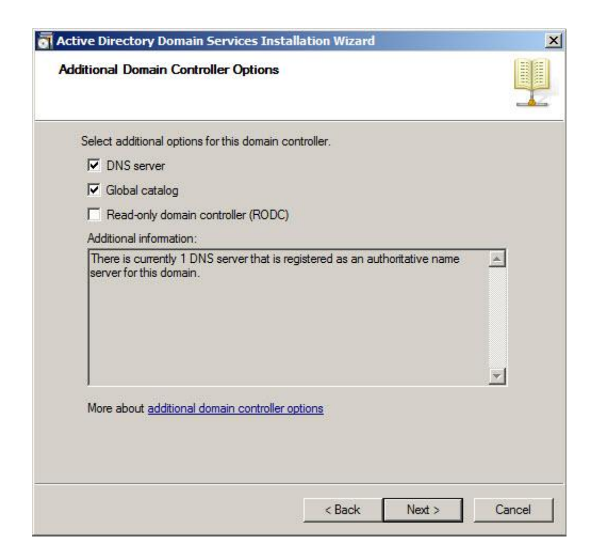


هنختار اول اختيار Existing Forest عشان انا عندي Forest طبيعي

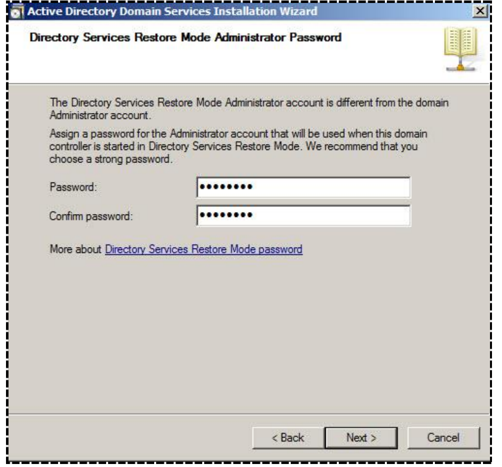


هنحط اسم الDomain بتاعنا الرئيسي وال credential بتاعه الadministrator

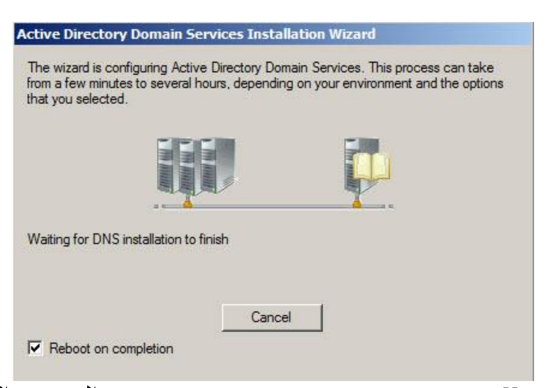
Next → Next



هنا يكون تنزيل الDNS Server والGlobal Catalog أختياريا .. ويفضل ان يتم تنزيلهم حتي يكون كل Domain مختص بذاته
ومن هذه الواجهه يمكنني ان اختار Read-Only Domain Controller (سنتعرف عليه لاحقا)



دي كلمه السر بتاعه ال Restore mode زي ما اتكلمنا قبل كدا



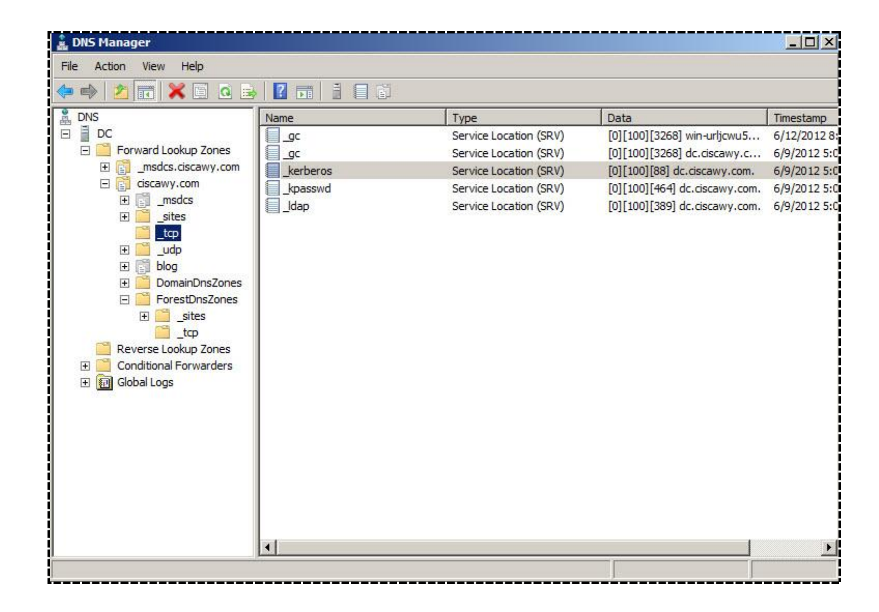
ستجد ان الصوره الخاصه بال Installation متغيره وهي تنسخ من Domain الرئيسي اليDomain إضافي اما الصوره الخاصه بأول Domain كانت كتابه فقط
يمكن ان ترجع لها في الشابتر الخاص بها

- ✓ بعد عمليه اعاده التشغيل

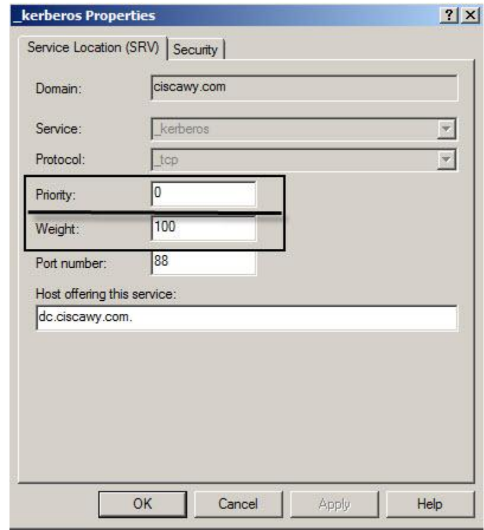
قم بفتح .. Start → Administrative tools → Active directory Users and Computer
قم بانشاء اي Object علي ال Additional Domain
قم بعمل Refresh سريع علي الDomain الرئيسي ستجد ان الObject موجود

- ✓ في حالة اذا اردت ان يكون أين من ال Two Domains له الاولوية في الاستجابة والغاء موضوع الـ Load Balancing

علي أي منهما ونقوم بفتح Start → Administrative tools → DNS



Double Click on Kerberos→ البروتوكول المسئوال عن عمليه الوثوقيه



نقوم بتغيير اي من قيمه ال Priority او قيمه ال Weight

- ✓ في هذه الحاله لن تكون الاستجابه بالتناوب ولكن ستكون الأولويه لصاحب القيمه الأعلي

Read Only Domain Controller "RODC"

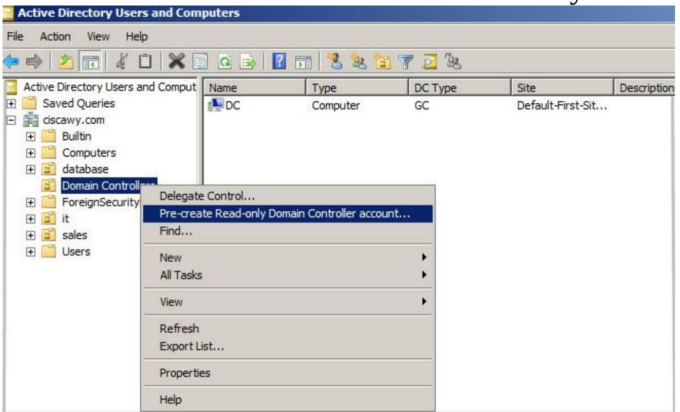
- ✓ نفس فكره ال Additional domain
- ✓ يستخدم الRODC كنسخه للقراءه فقط من الDomain الرئيسي
- ✓ يستخدم كنوع من انواع الحمايه الداخليه للشركه الخاصه بي حيث انه لا يقوم يحفظ كلمات المرور فإن حدث اي اختراق للDomain الخاص بي لن يتم سرقه ال Passwords
- ✓ يستخدم ايضا اذا كان في احدي فروع الشركه مدير IT ولكنه لا زال جديدا في شركتي ففي هذه الحاله اقوم بإنشاء Domain للقراءه فقط حفاظا علي البيانات وكلمات المرور الخاصه بشركتي

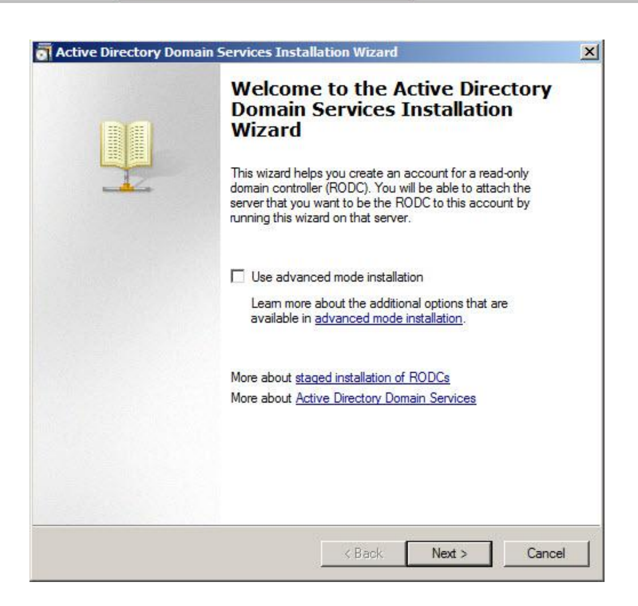
- ✓ Provide valuable support for branch office scenarios by authenticating users in the branch office.
- ✓ RODCs reduce the security risk associated with placing a domain controller in a less secure site.
- ✓ You can configure which credentials an RODC will cache.
- ✓ You can also delegate administration of the RODC without granting permissions to other domain controllers or to the domain.

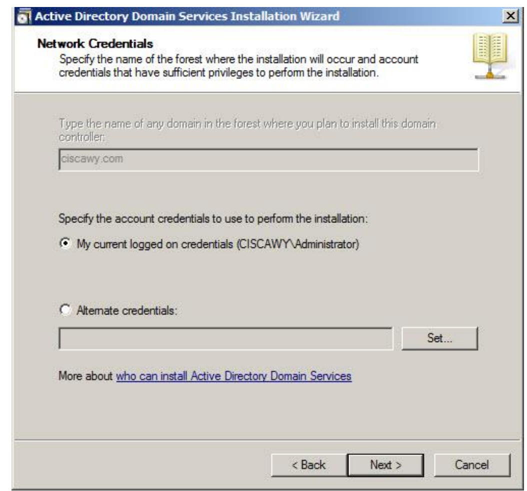
علي الMachine اللي عليها الDomain الرئيسي ciscawy.com

Start → Administrative tools → Active directory users and computers

R.click on Domain Controllers → Rre-create Read Only Domain Account

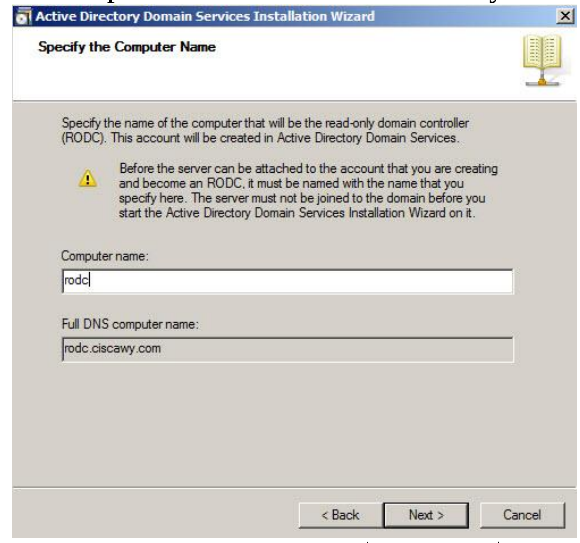




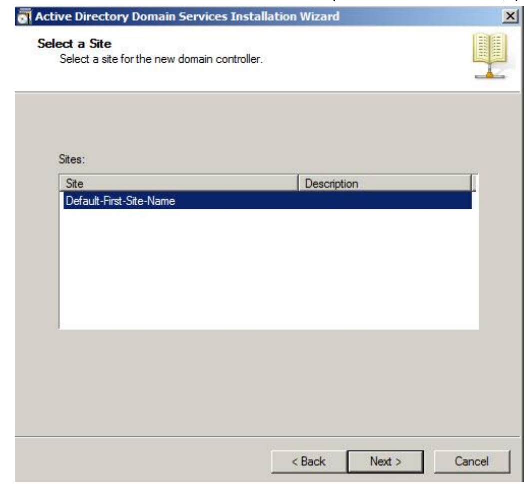


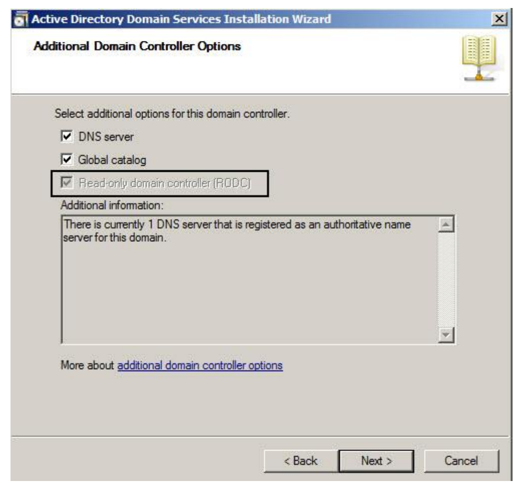
الUser اللي ليه صلاحيات انه ينشأ الRODC

هنسيبها زي ما هيا My Current Logged عشان انا داخل بالEnterprise Admin

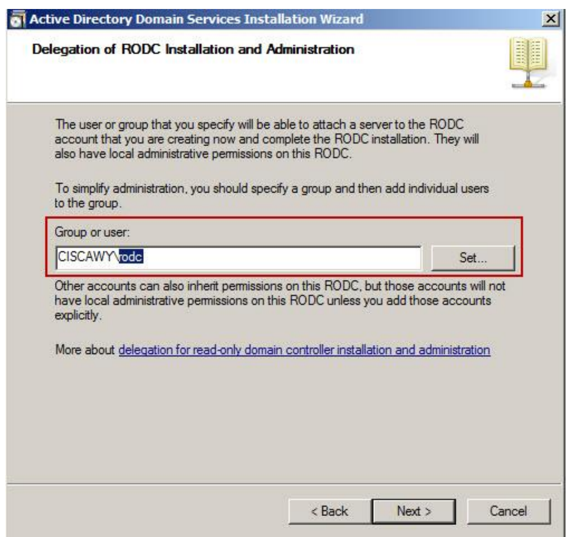


دا اسم الجهاز اللي هنقوم بعمليه تنصيب الRODC عليه



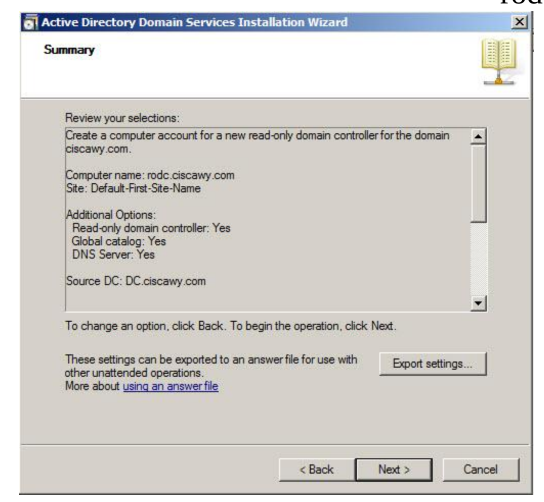


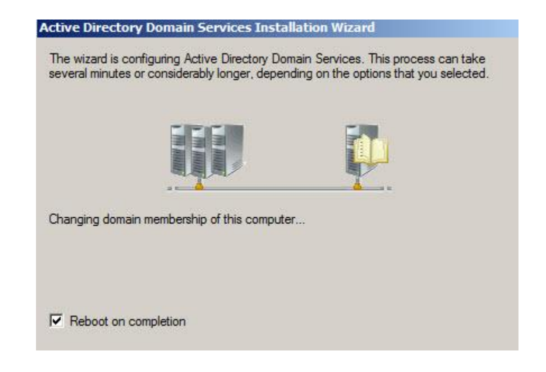
هنلاقي هنا RODC اتفعلت و هنترك ال DNS & GC



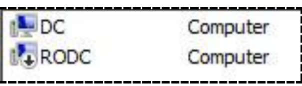
هنختار هنا مين الUser او الGroup اللي هيكون ليهم الصلاحيات انه يعمل Logon علي الRODC ويقدروا يشوفوا الDatabase الخاصه بيه

قد قمت مسبقا بإنشاء User اسمه rodc





وبعد كدا هنضغط علي Finish

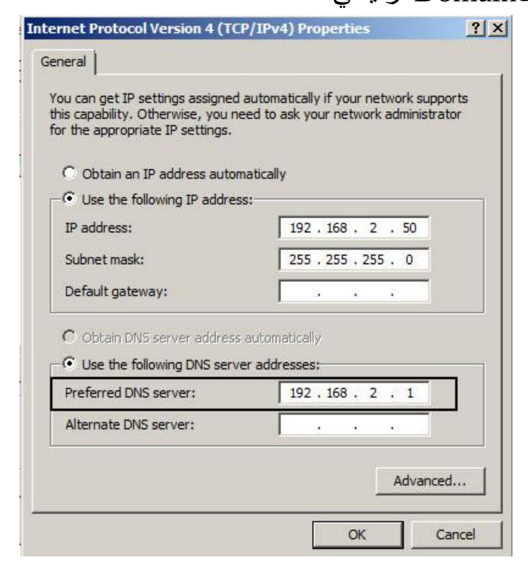


سنجد ان icon الخاصه بالكومبيوتر الrodc لها شكل مختلف

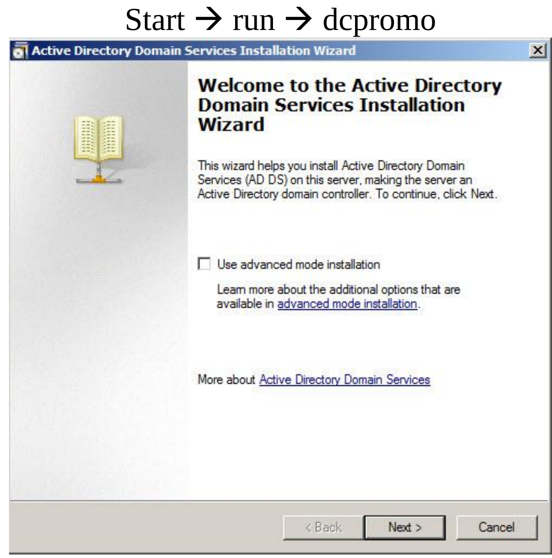
علي الmachine الثانيه المسماه RODC

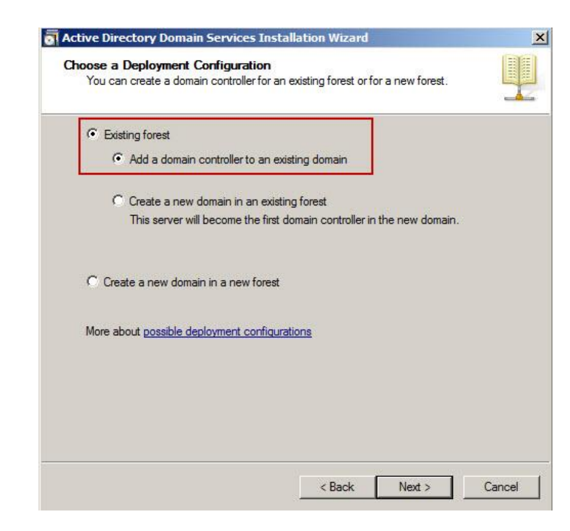
اعدادات الTCP/IP

الGateway هو الIP الخاص بالDomainالرئيسي



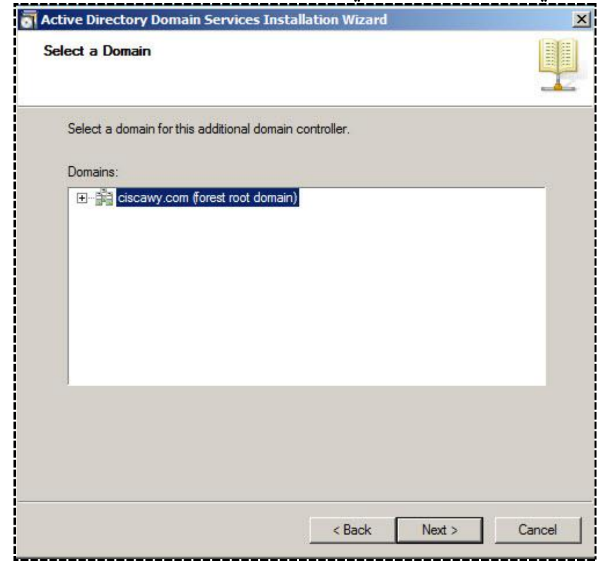
Start → run → dcpromo

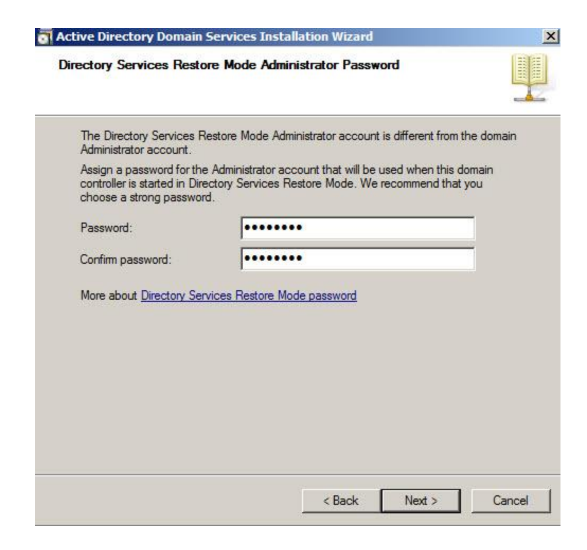




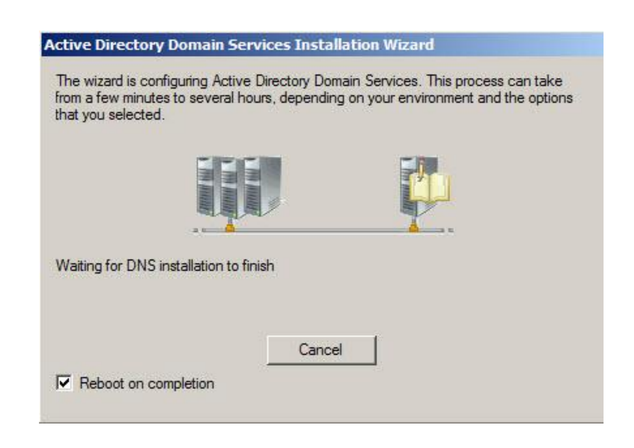
Next → Next

هندخل اسم الForest الرئيسيه بتاعتنا
والCredential الخاصه باليوزر اللي انا كنت ضايفه في الاعدادات السابقه

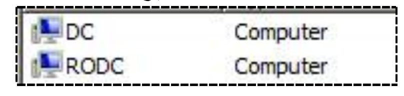




Next → Install

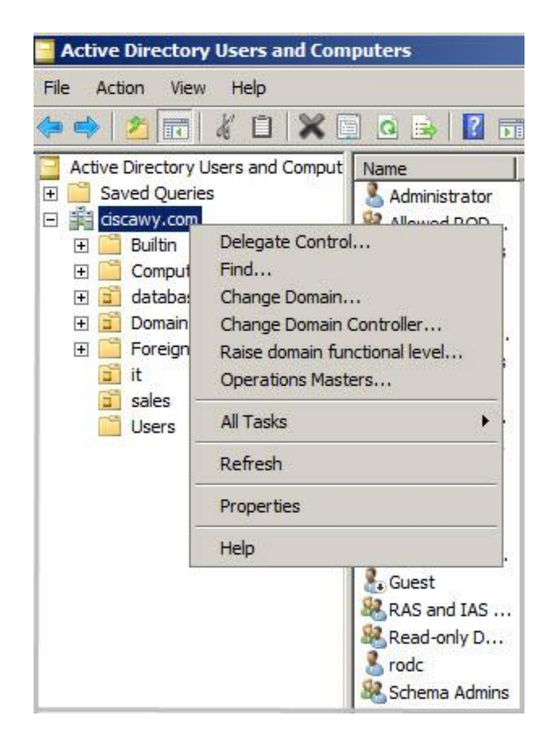


بعد عمليه اعاده التشغيل سنجد ان الIcon الخاصه بالRODC تغيرت

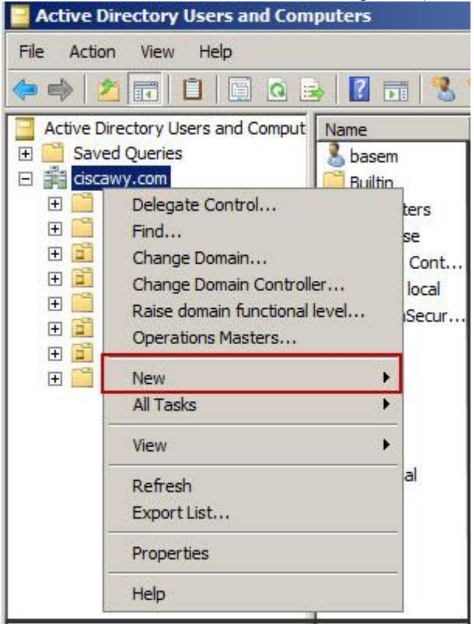


- لا يقوم الRODC يحفظ كلمات المرور ،، لذلك اذا اراد اي مستخدم ان يقوم بالدخول علي الRODC يتم الاتصال بالDomain الرئيسي حتي يحصل علي التصريح المخول له للدخول
- ولكن يمككنا السماح لبعض الUsers بعمل cache لكلمه المرور الخاصه بهم علي هذا الDomain حتي نقلل الاستهلاك ونحد من ال Delay
- لا يسمح لأحد بان يقوم بإنشاء اي Object علي الRodc حتي من صرح له بالدخول اليه
- فقط الEnterprise Administrator هو من يملك التصريح

عند الدخول باليوزر المسمي RODC الذي تم اضافته في عمليه الإعدادات



لا توجد هنا كلمه NEW الخاصه بانشاء اي object جديد

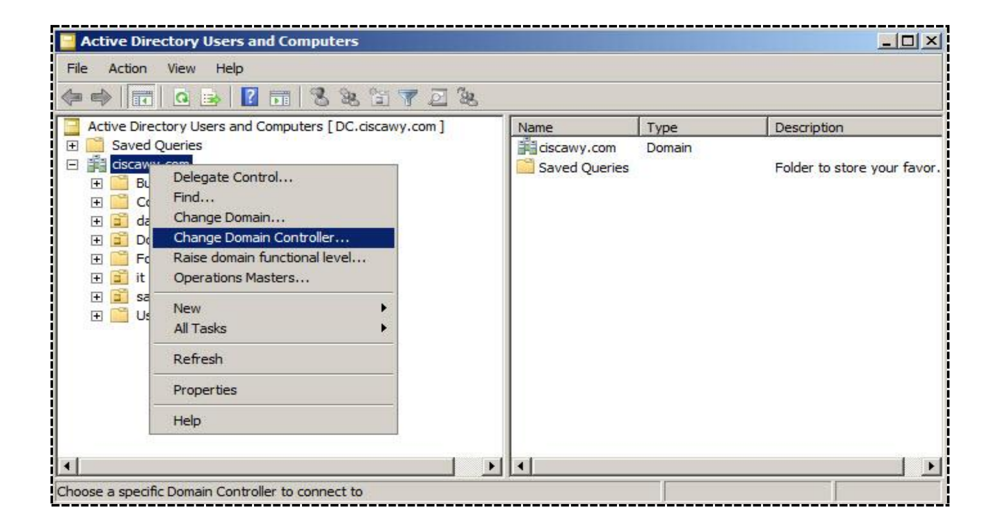


عند الدخول بحساب الEnterprise Administrator سنجد قائمة New متاحه لنا

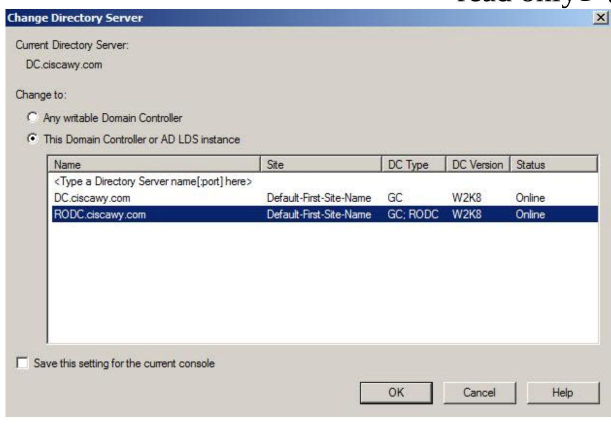
ملاحظه هامه جدا

حينما تقوم بالدخول الي الDomain المخصص للRead Only ستجد انك علي الDomain الرئيسي للقيام بالدخول علي الRODC

R.click on Domain Name → Change Domain Controller



ونختار الDomain المخصص لread only





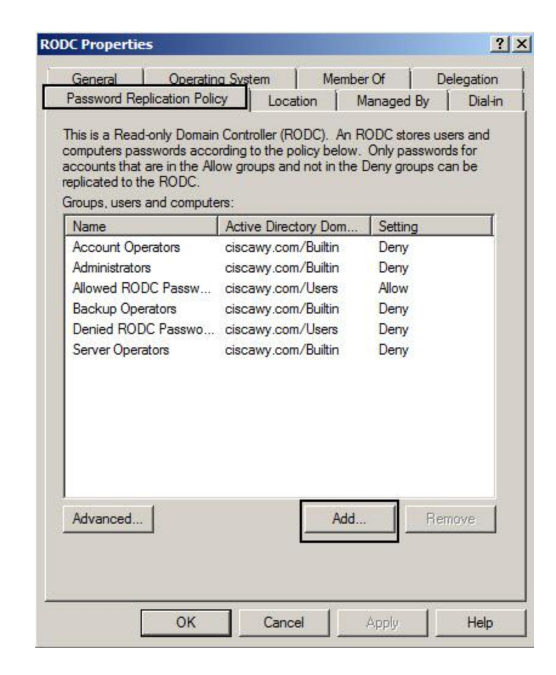
اي ان هذا الDomain هو للقراءه فقط ولن تستطيع ان تضيف له اي object حتي وان كنت مدير هذا الDomain

- سيحدث تضاعف تلقائيا Replication بين الDomain الرئيسي والRODC
- أي ان حينما اقوم بانشاء اي Object علي الDomain الرئيسي سيححدث له تضاعف علي الRODC

- **هل من مصرح لهم** بالدخول علي الRODC يكون الDomain الرئيسي متاح حتي يستطيعوا ان يدخلوا عليه !!

بالطبع لا ، فنحن يمكن لنا السماح بتضاعف كلمه المرور الخاصه بهم علي الDomain الRead Only
Password Replication ويحدث لكلمه المرور الخاصه بهم Cache علي الRODC
علي الجهاز الخاص بالRODC

Start → administrative tools → active directory users and computers
Open domain controller's container →R.click on RODC → properties

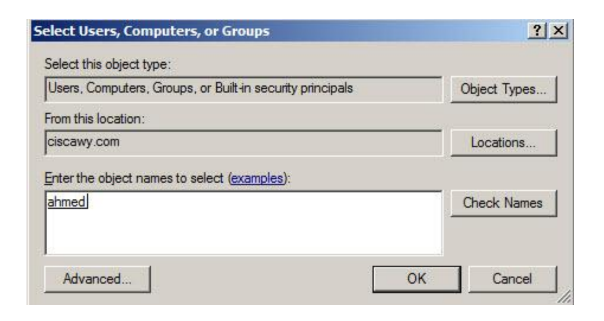


ونختار Password Replication Policy ← ونضغط علي Add

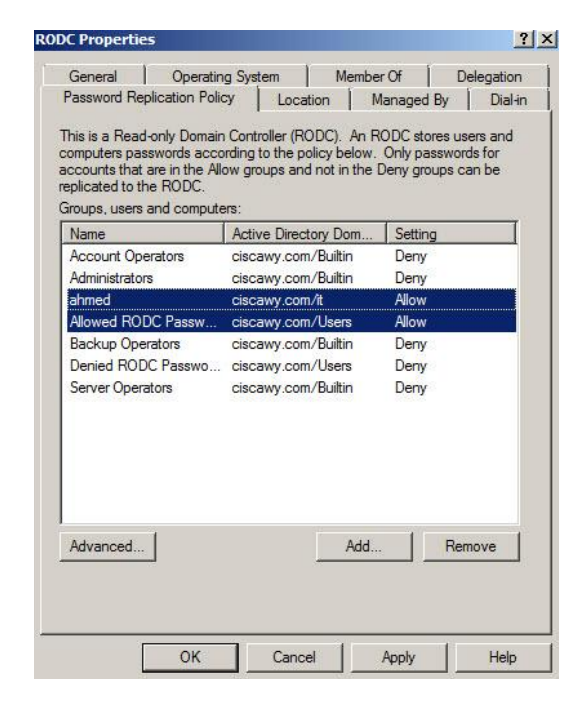


واختار علي حسب اللي انا عايز اليوزر يعمله سواء deny او allow

في هذه الحاله هختار Allow



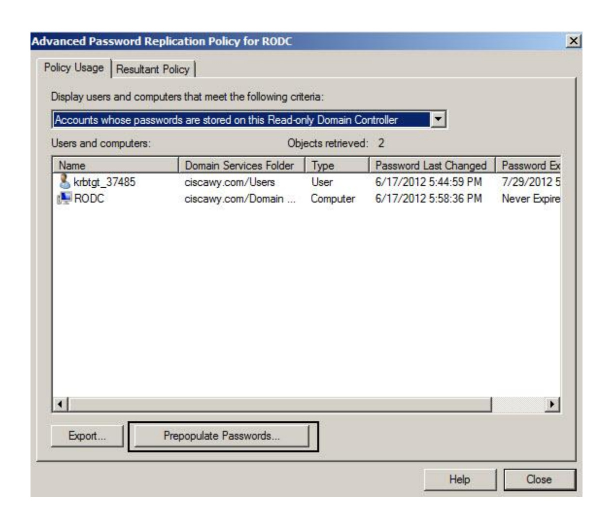
وبعد كدا هعمل ok



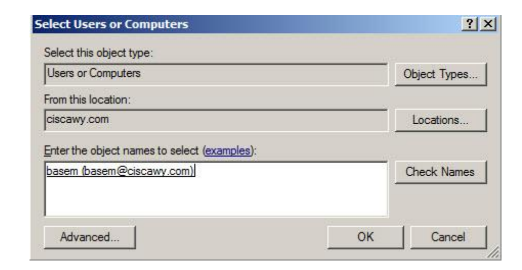
- سنجد هنا ان فقط ahmed المضاف الان و rodc الموضوع من قبل allow والباقي deny
- اي هم فقط من يستطيعوا ان يدخلوا علي ال Read Only Domain Controller

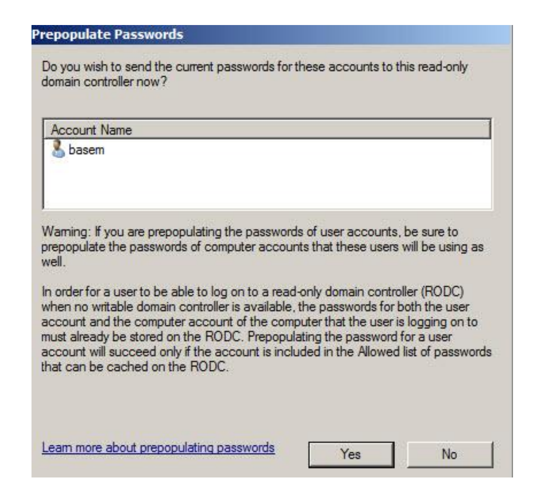
- حتي نختار مجموعه من الUsers يتم عمل Cache للكلمه المرور الخاصه بهم علي الRODC
- لغرض انه حينما يقوم بالدخول عليه يتم اخد الوثوقيه من هذا الDomain
- أي ان كلمه المرور الخاصه بهم سيتم تخزينها علي الRODC

نختار Advanced



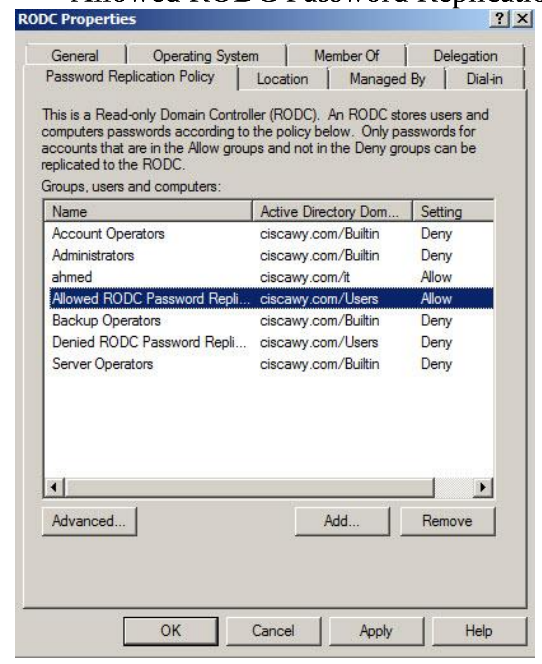
ثم نضغط علي prepopulate password





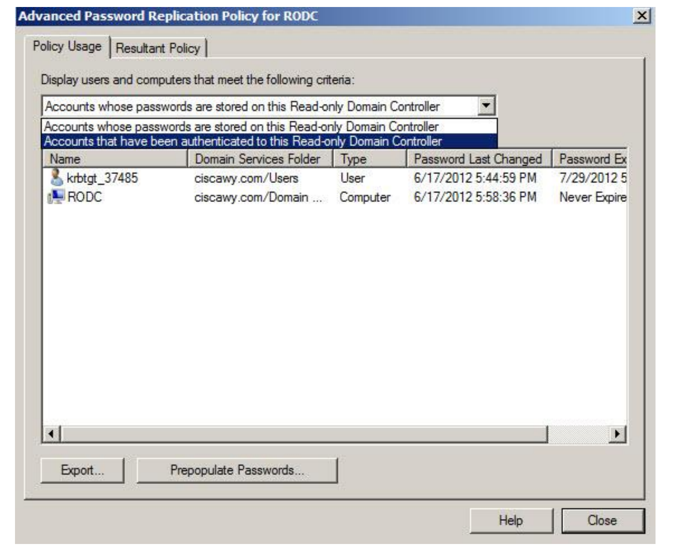
ال Replication :-

نقف علي القائمه المخصصه بال Allowed RODC Password Replication

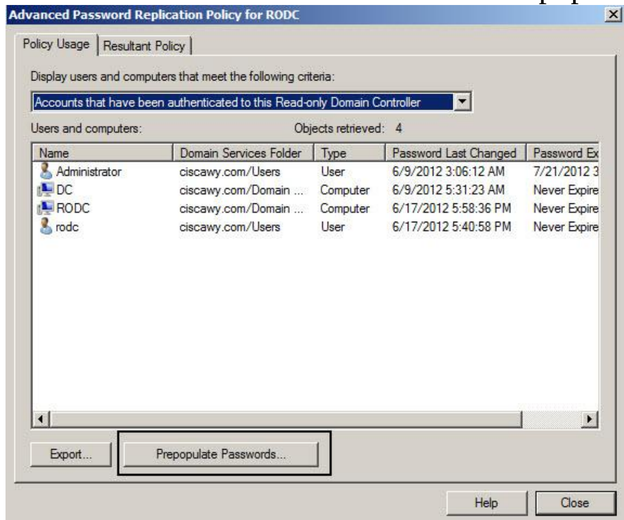


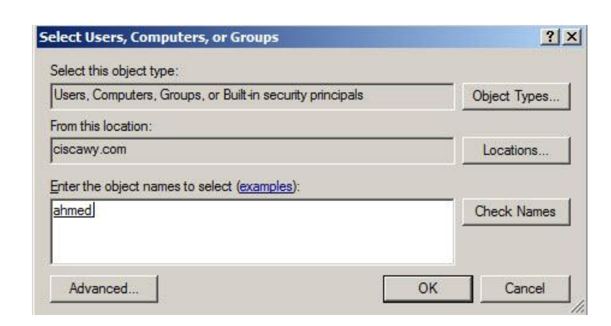
نختار Advanced

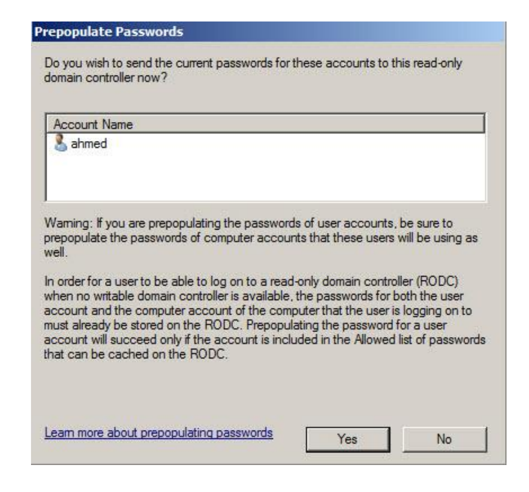
ثم نختار الثانيه ← Account has been Authenticated



ثم نضغط علي Prepopulate Password







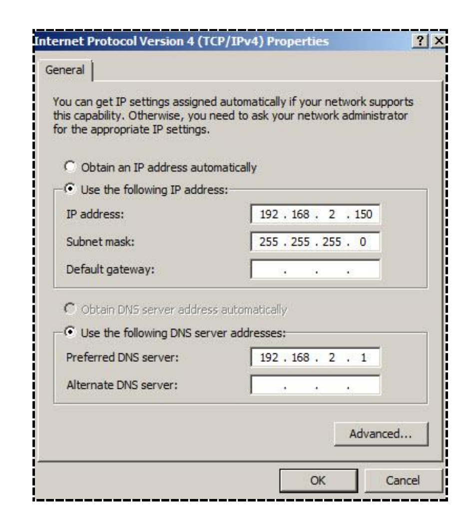
بعد هذا ،،

اذا قمت بالدخول الي الRead Only Domain Controller باليوزر المدعوahmed والاتصال بين ال Two Domains مفصول ستجد انه يستطيع ان يدخل الي هذا الDomain

Child Domain

- الغرض منه هو ان يكون لدي في مؤسستي Domain صغير من الDomain الرئيسي Sub-Domain
- قد تكون مؤسستي تزايد عدد الUsers بها وتنوعت النشاطات وزادت التخصصات،، في هذه الحاله اقوم بإنشاء Domain صغير من الDomain الرئيسي يكون المتحكم فيه هو الEnterprise Administrator ولكن له Database خاصه به
- يتم انشاءه علي Machine منفصله عن الDomain الرئيسي
- ليس كالRODC or Additional حينما اقوم بانشاء اي Object يتم تضاعفه ،، لا ! فهذا الDomain منفصل في كل شئ وله Database خاصه به كما قلت
- ولكن يكون التحكم فيه عن طريق الEnterprise Administrator

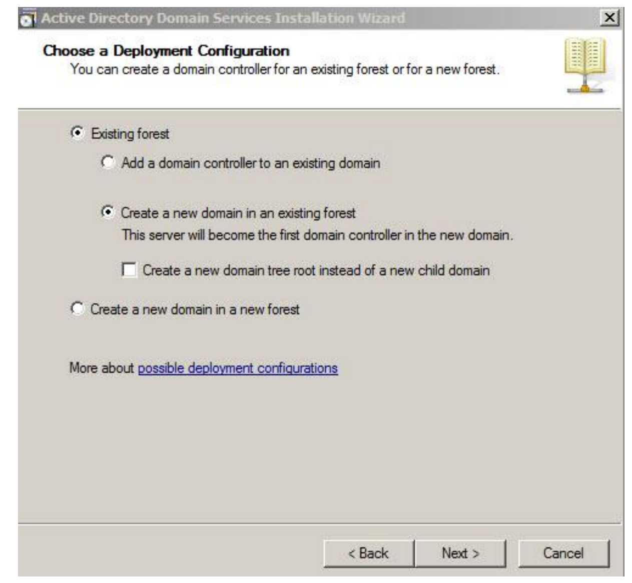
اعدادات الTCP/IP



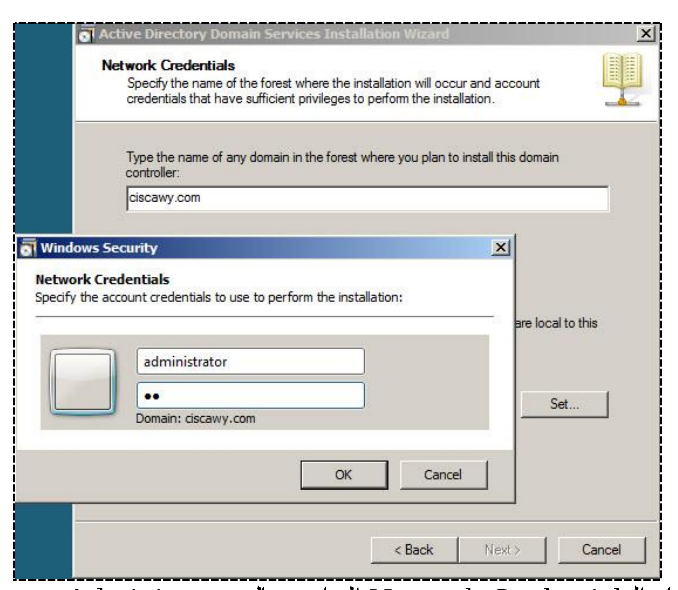
Start → run → dcpromo



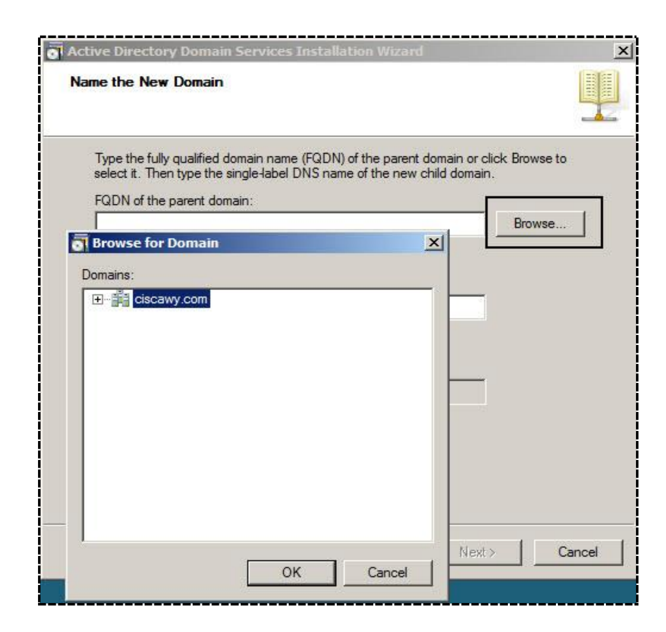
لقد تعودنا علي هذه الشاشه ☺
في هذه المرة سنستخدم ال Advanced mode



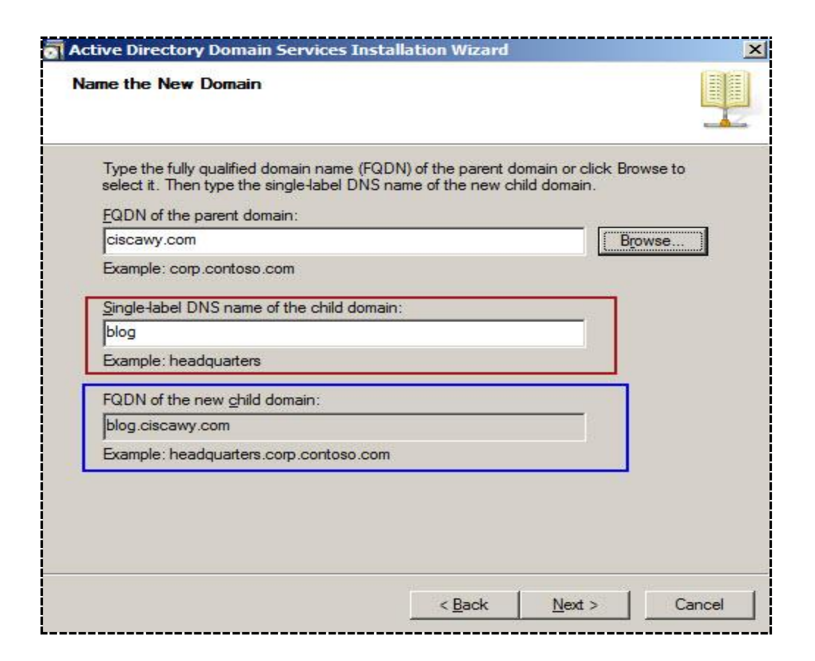
هنختار الاختيار التاني New Domain in an Existing Forest



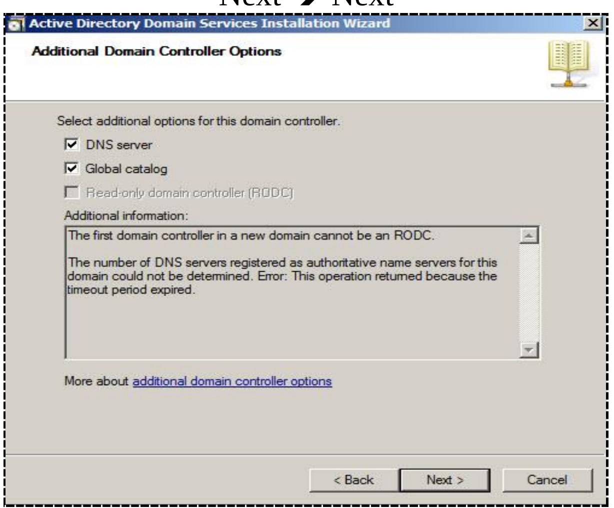
اسم الForest الخاصه بنا و الNetwork Credential الخاصه بالAdministrator



هنضغط علي Browse ونختار الDomain ثم نقوم بكتابه اسم ال Child Domain الجديد



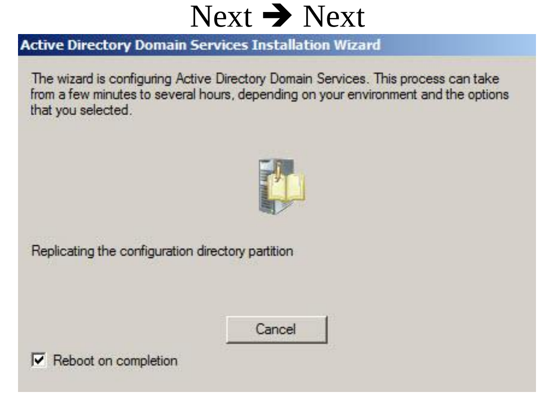
Next ➔ Next



الGlobal Catalog هنا يكون اختياريا ولكن يفضل تنزيله

ويفضل ايضا ان يكون له الDNS الخاص به حتي لا يحدث اي load علي الDomain الرئيسي

Next ➔ Next



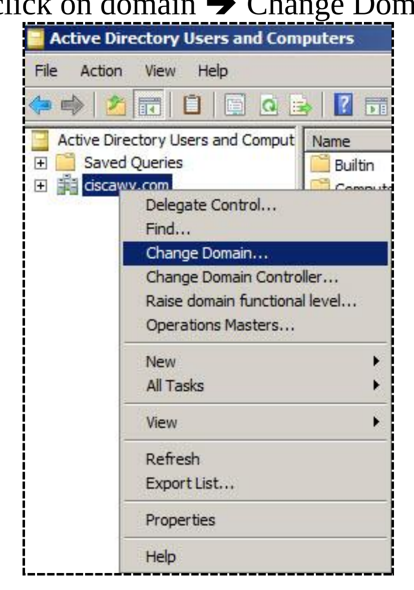
- بعد عمليه اعاده التشغيل ستجد ان كل من الDomain الرئيسي والChild Domain كل منهما له Database خاصه به
- ولا يحدث اي تضاعف بينهما حينما اقوم بإنشاء اي Object علي اي منهما

- مدير النظام الخاص فقط بالChild domain لا يستطيع ان يقوم بالتحكم في الDomain الرئيسي ،، انما يحدث العكس

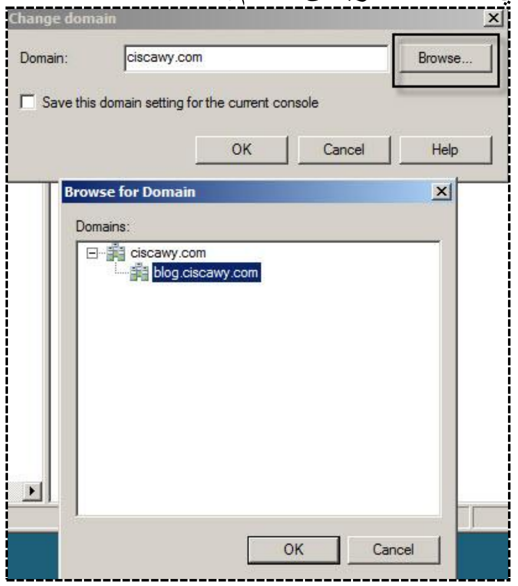
بعض الملاحظات الهامة:-

- علي الDomain الرئيسي يمكنك ان تتنقل من بين هذا الDomain وأي Domain اخر في الForest عن طريق ،،

Start → administrative tools → active directory users and computers
R.click on domain ➔ Change Domain



بعد كدا نختار Browse ونختار اي Domain نريد ان نتحكم به

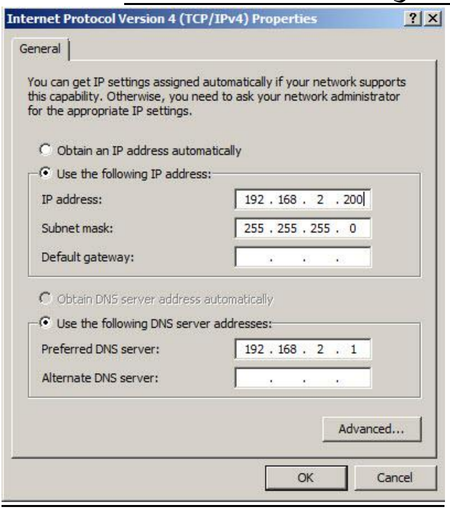


- يمكنك ان تقوم بالعمليه العكسيه من علي اي Domain سواء كان Child او New Tree ان تتحكم في الDomain الرئيسي **شرط** ان تكون **Enterprise Administrator** بنفس الطريقه
- يمكن لل**Enterprise Administrator** أن يقوم بالتعديل سواء كان بالاضافه او بالحذف من علي الDomain الرئيسي والChild
- نوع الTrust بين الDomain الرئيسي والChild تكون في الغالب Two way - بمعني ان الثقه متبادله - أي ان يستطيع اي من ال**Enterprise Administrator** الخاص بكل منهما التعديل في الاخر
- يمكني ان اقوم بأنشاء Child Domain جديد من الChild الرئيسي ،، اذا كانت مؤسستني في حاله توسع مستمر

New Tree Root

- نستخدم هذه الخدمة حينما نقوم مؤسستي بالتعاقد مع شركة أخري وأريد ان يكون كل شركة (Domain) له المستخدمين الخاصين به
- اي يكون لكل شركه قاعده البيانات الخاصه به ولكن تتم ادارتهما عن طريق مدير نظام واحد فقط
- أو بمعني آخر اريد ان يكون كل Domain له الDatabase الخاصه به ويتحكم فيهما **Only One Enterprise Administrator**
- كل شركه لها اسم الDomain الخاص بها :-
  - لنفترض ان هناك شركتان A & B وكل منهما له مستخدمين
  - المستخدمين يكونوا الUPN الخاص بهم user@B.com , user@A.com
  - فانا اريد ان يظلوا هكذا حتي بعد الشراكه وتكون ادارتهم عن طريق Domain واحد فقط بـ Enterprise Admin واحد

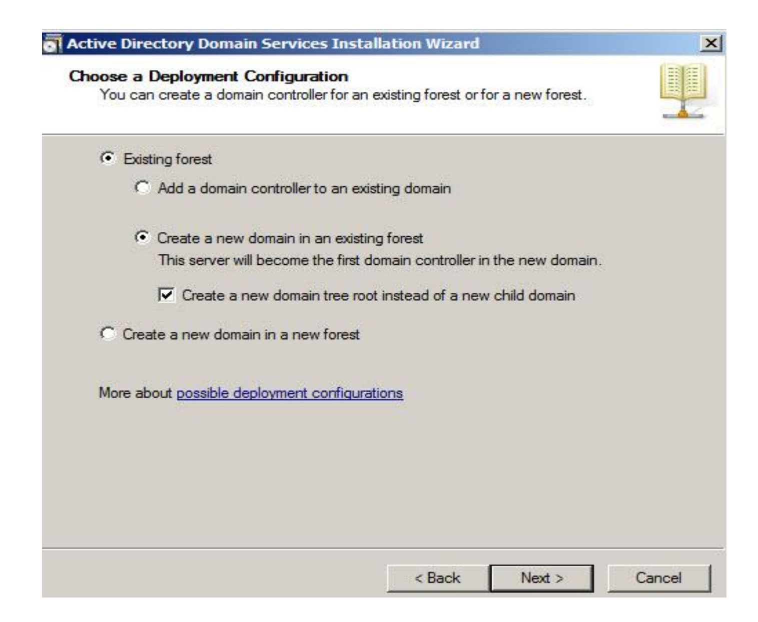
طريقه اعدادات الTCP\IP علي المكنة المراد انشاءها كـ New Tree



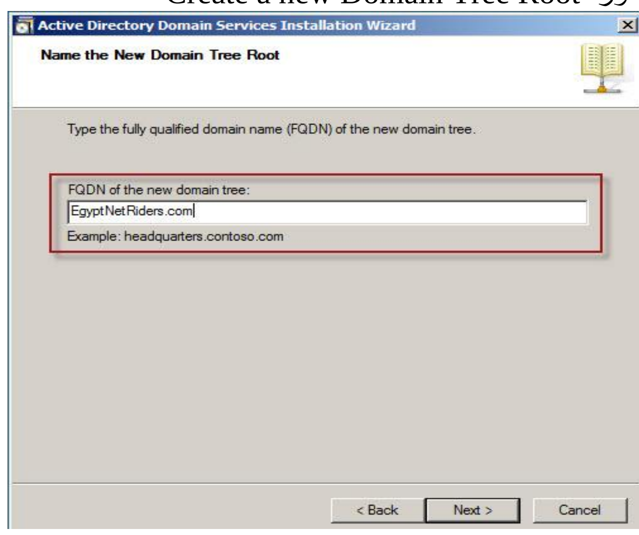
بعد ذلك

Start → run → dcpromo

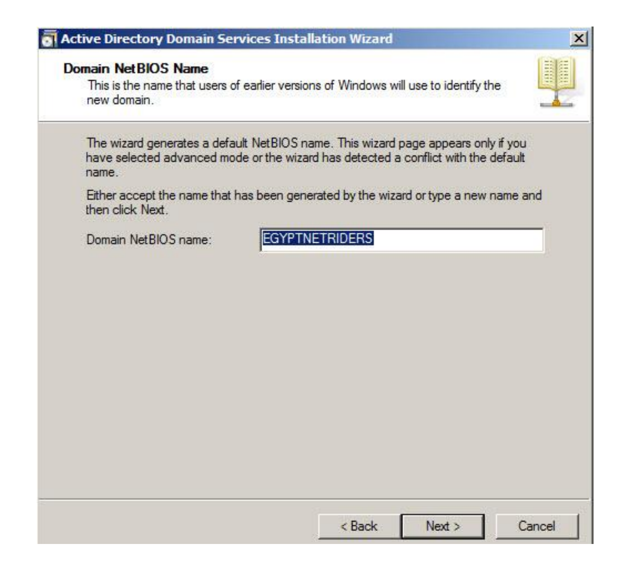




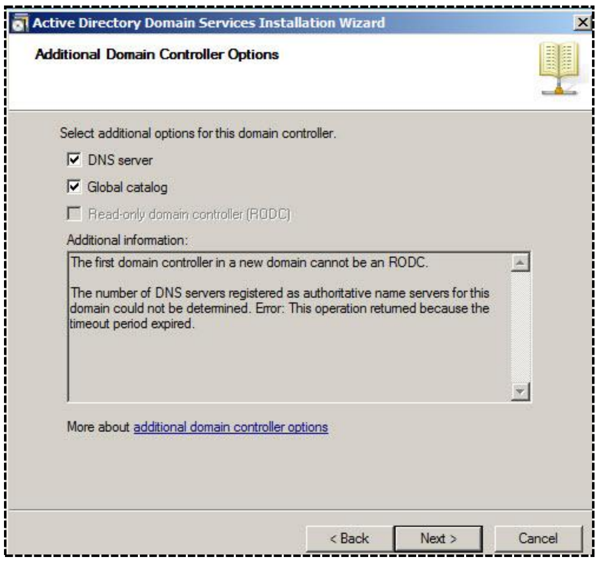
سنختار كما هو موضح في الصورة Create a new Domain Tree Root

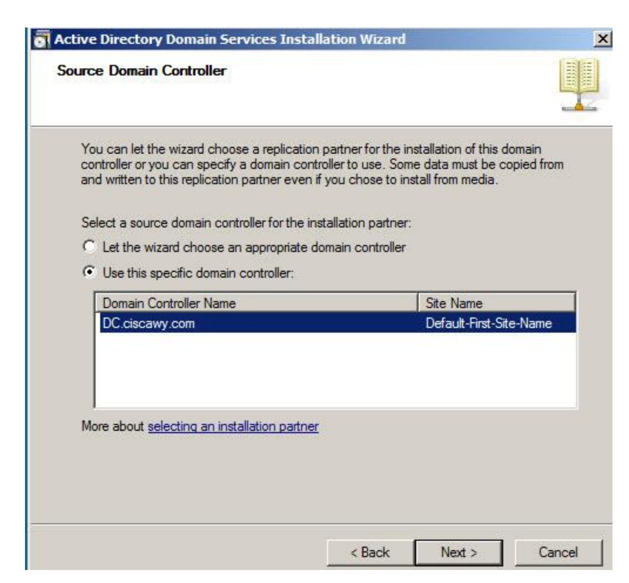


- هنا يتم اختيار اسم الTree الجديده او اسم المؤسسه التي تعاقدنا معها
- ليس شرطا ان تكون نفس اسم الDomain الرئيسي كما حدث في الChild لذلك تجد انه ليس هناك اختيار لكي تقوم بعمل Browse
- يتم اختيار اي اسم جديد للDomain الجديد
- فقط ارتباطه بالDomain الرئيسي في الأدارة فقط لا غير

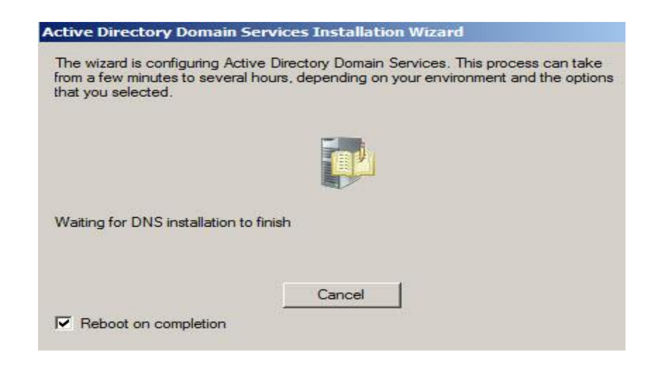


يفضل ان يتم انزال الـDNS & GC كما تعلمنا من قبل





Next ➔ Next

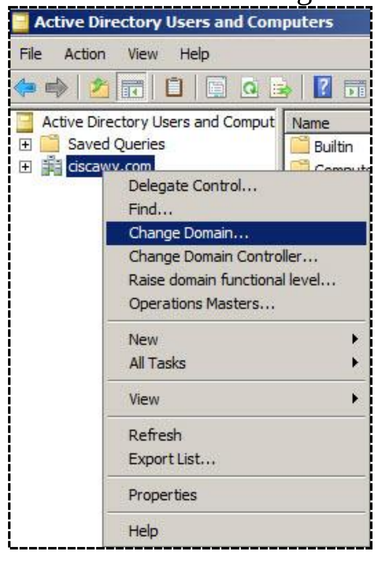


- بعد عمليه اعاده التشغيل ستجد ان كل من الDomain الرئيسي والNew TREE كل منهما له database خاصه ومنفصله
- ولا يحدث اي تضاعف بينهما حينما اقوم بإنشاء اي Object علي اي منهما

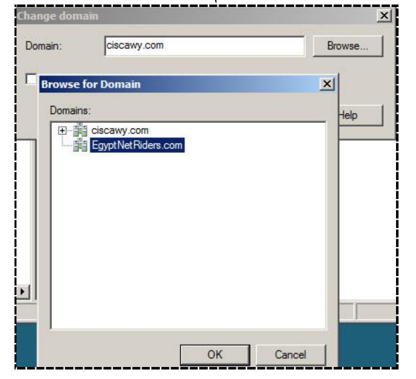
بعض الملاحظات الهامة:-

- علي الDomain الرئيسي يمكنك ان تتنقل من بين هذا الDomain وأي Domain اخر في الForest عن طريق ،،

Start → administrative tools → active directory users and computers
R.click on domain → Change Domain



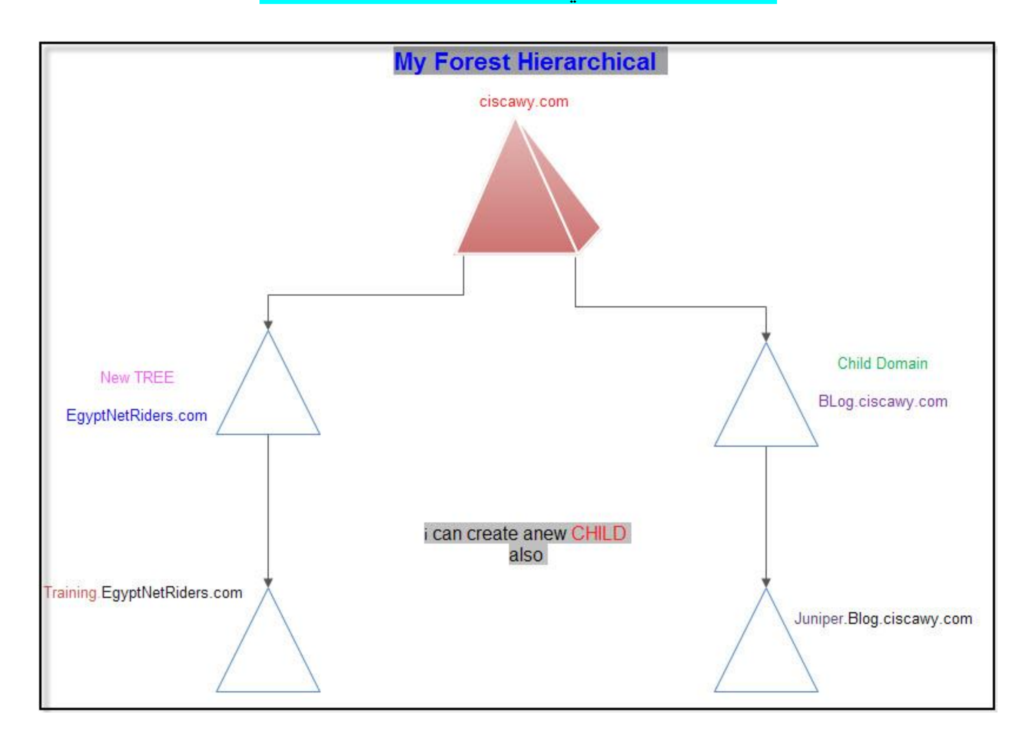
بعد كدا نختار Browse ونختار اي Domain نريد ان نتحكم به

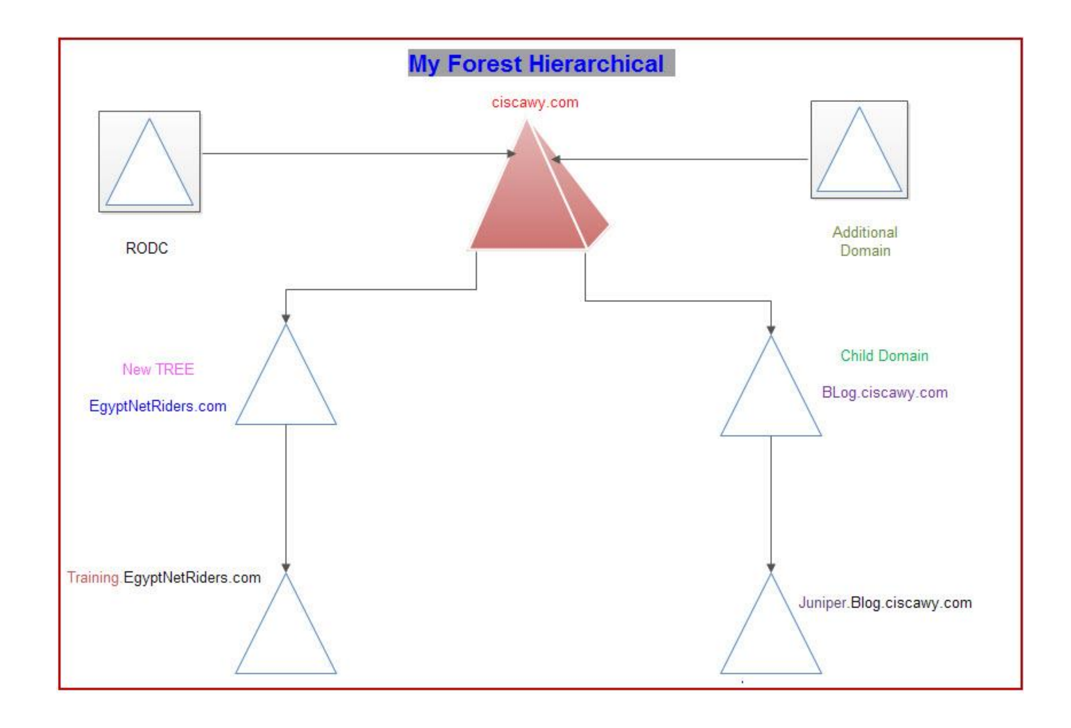


- يمكن للEnterprise Administrator أن يقوم بالتعديل سواء كان بالاضافه او بالحذف من علي الDomain الرئيسي والNew TREE

- نوع الTrust بين الDomain الرئيسي والNew TREE تكون في الغالب Two way - بمعني ان الثقه متبادله - أي ان يستطيع اي من الEnterprise Administrator الخاص بكل منهما التعديل في الاخر
- يمكني ان اقوم بأنشاء Child domain جديد من الTREE الجديده ،، اذا كانت مؤسستني في حاله توسع مستمر

هذا الشكل التوضيحي يلخص ما قد تحدثت عنه سابقا





Active Directory Partition (Database)

قاعده البيانات الخاصه بالActive Directory

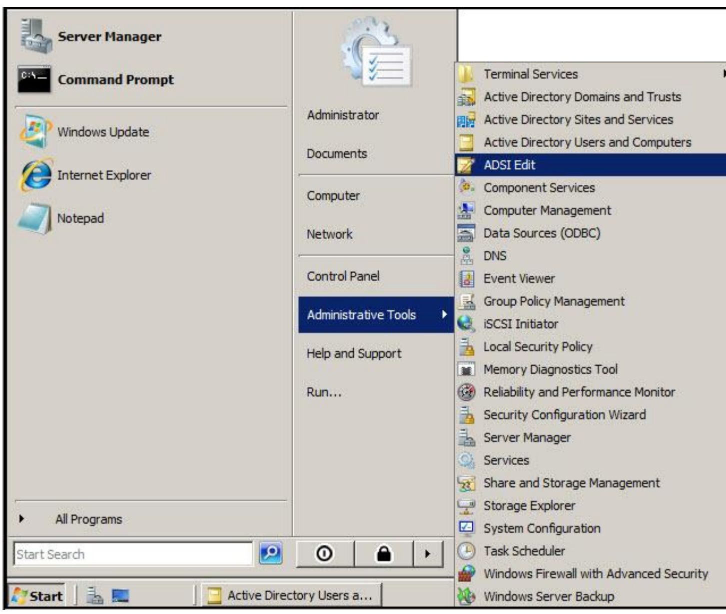
- اثنين علي مستوي الForest :- اي انه لا يوجد إلا Partition واحد فقط في Forest
- اثنين علي مستوي الDomain:- اي ان كل Domain له الPartition الخاص بي

Forest Level	Domain Level
1- Schema Partition	1- Domain Partition
2- Configuration Partition	2- Application Partition

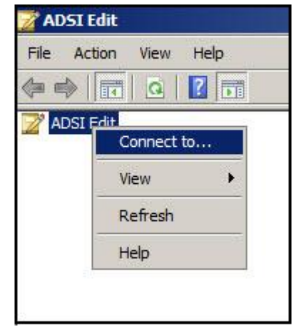
١- Schema Partition

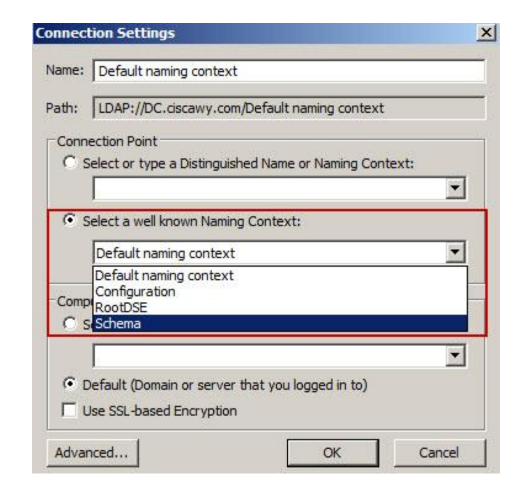
- تحتوي علي كل المعلومات الخاصه بالObject والAttribute الخاصه بهم
- لإجراء اي تعديلات عليها (not recommended) لا بد من ان يكون Enterprise administrator لأن اي خطأ ممكن ان يؤدي الي حدوث failure في النظام ككل
- لمعرفه مكان هذا ال partition :-

Start → administrative tools → ADSI edit

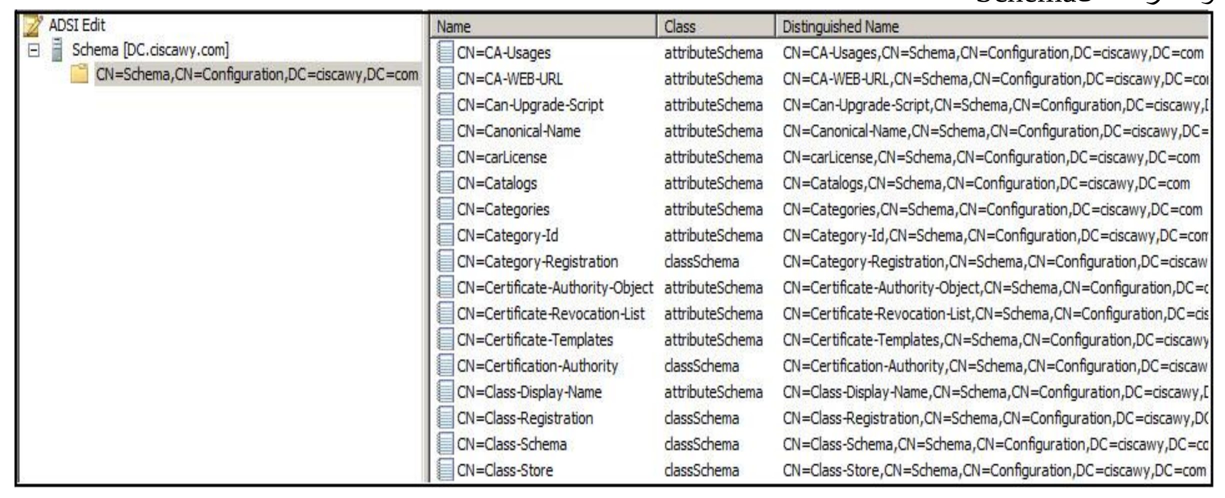


R.click → Connect to





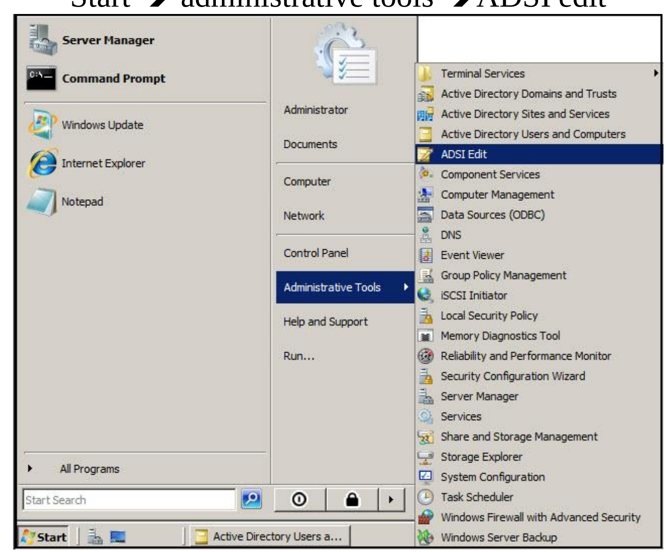
ونختار هنا الSchema



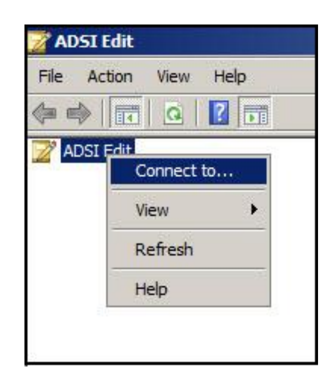
٢- Configuration Partition

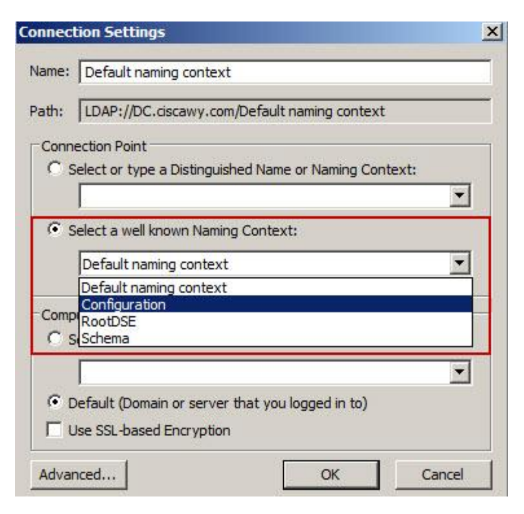
- تحتوي علي معلومات عن البنيه التحتيه infrastructure الخاصه بالفورسيت
- كل المعلومات عن الsites و الip الخاص بكل سايت وطريقه الreplication بينهما
- لمعرفه مكان هذا ال Partition :-

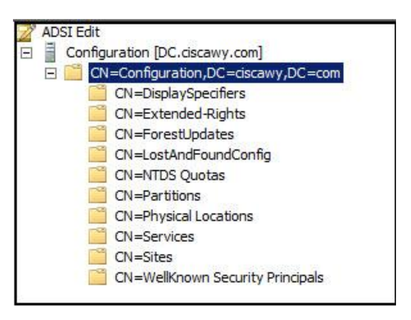
Start → administrative tools →ADSI edit



R.click → Connect to

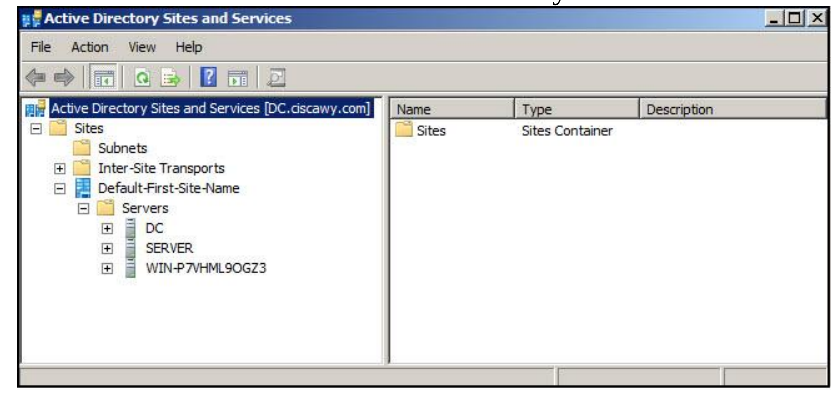






- وهناك أيضا مكان تخزينها في

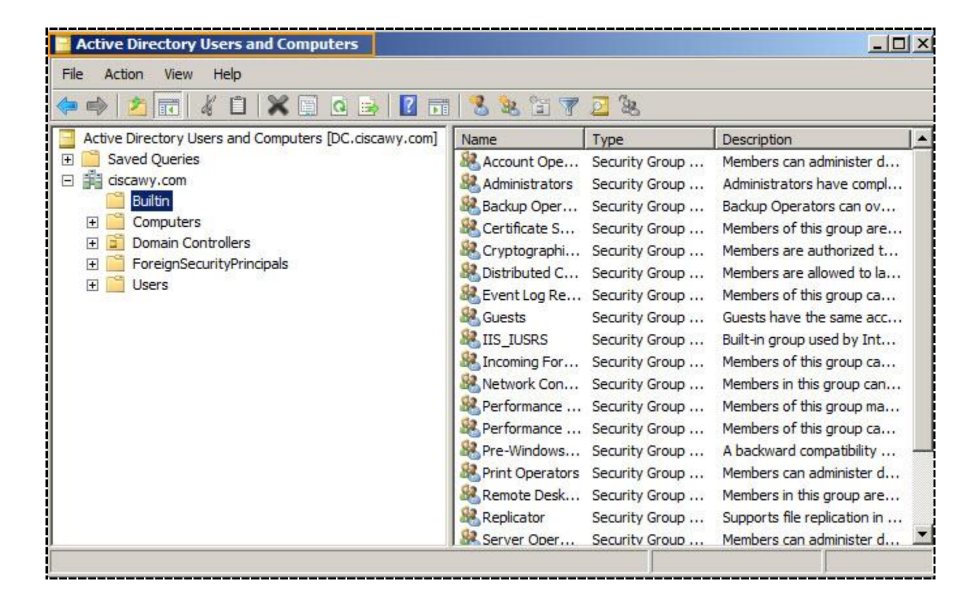
Start → administrative tools → Active Directory Sites and Services



٣- Domain Partition

- يحتوي علي كل ال Built-in Users and Computers. بكل خصائصهم Attribute & value
- تحفظ في :-

Active Directory User and Computers

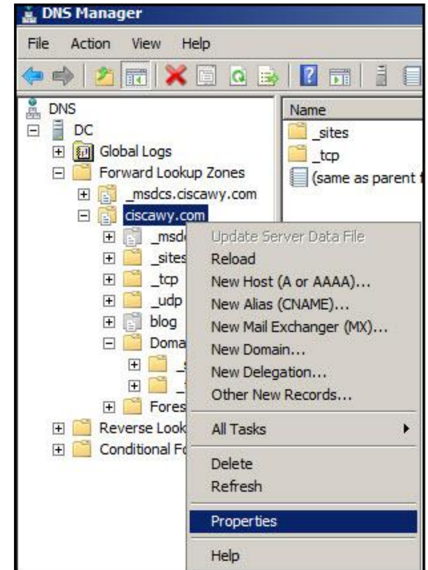


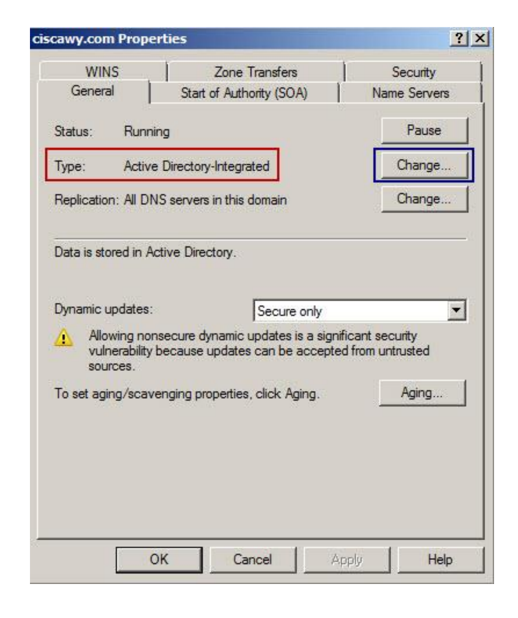
٤- Application Partition

- يحتوي علي اي Software لقاعده البيانات نحتاج اليها في الReplication
- كالDNS ان لم تكن مقتصره عليه
- Application partition → Active Directory Integrated Zone
- **انواع الDNS Zones (سنتعرف عليهم بالتفصيل في كورس الInfra)**

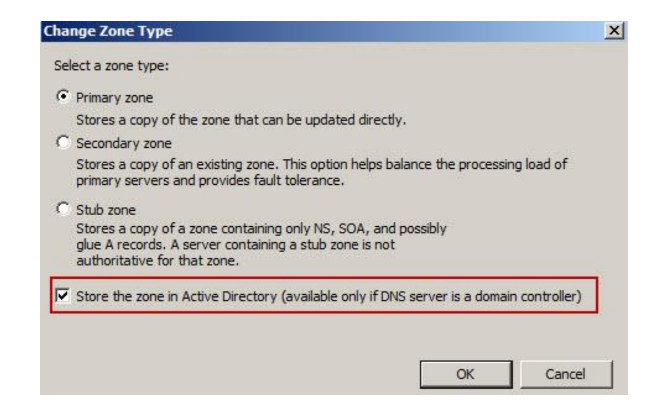
- Primary Zone
- Secondary Zone
- Stub Zone
- Active Directory Integrated Zone


Start → administrative tools → DNS





ثم نقوم بالضغط علي Change



- أي ان مكان تخزين الpartition الاخير هو الDNS

Five Operation Master Role
FSMO Roles

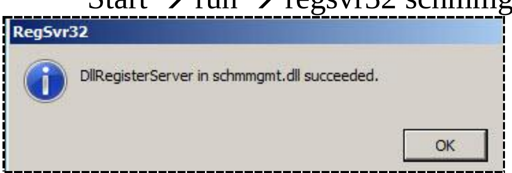
- Flexible Single Master Operation
- بعض الroles التي تسهل عمليه اداره الDomain
- تيسر عمليه المراقبه ومتابعه الاخطاء وتوزيع المهام الاداريه
- Five roles اثنان علي مستوي الForest أي يوجد منهما Role واحده فقط علي الforest
- وثلاثة علي مستوي الDomain اي ان كل Domain موجود له three role خاصه به

Forest Level	Domain Level
1- Schema Master Role **2- Domain Name Master**	1- Relative Identifier Master (RID) 2- Primary Domain Controller Emulator (PDC) **3- Infrastructure Master**

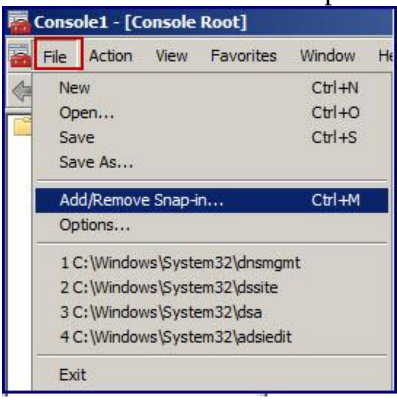
1- Schema Master Role

- تحتوي علي كل التحديثات والتعديلات التي تحدث علي مستوي الForest
- لمعرفه مكان تخزين هذه الrole :-

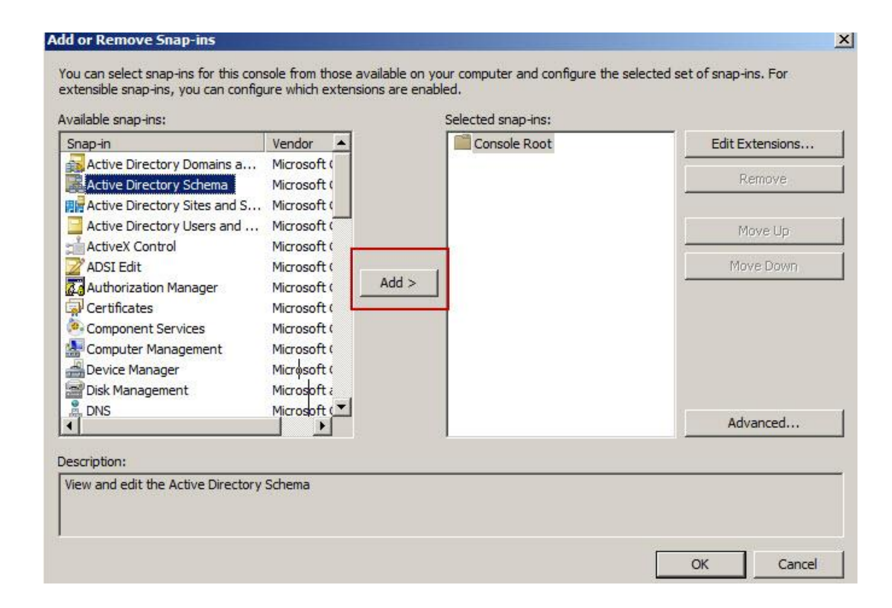
Start → run → regsvr32 schmmgmt.dll



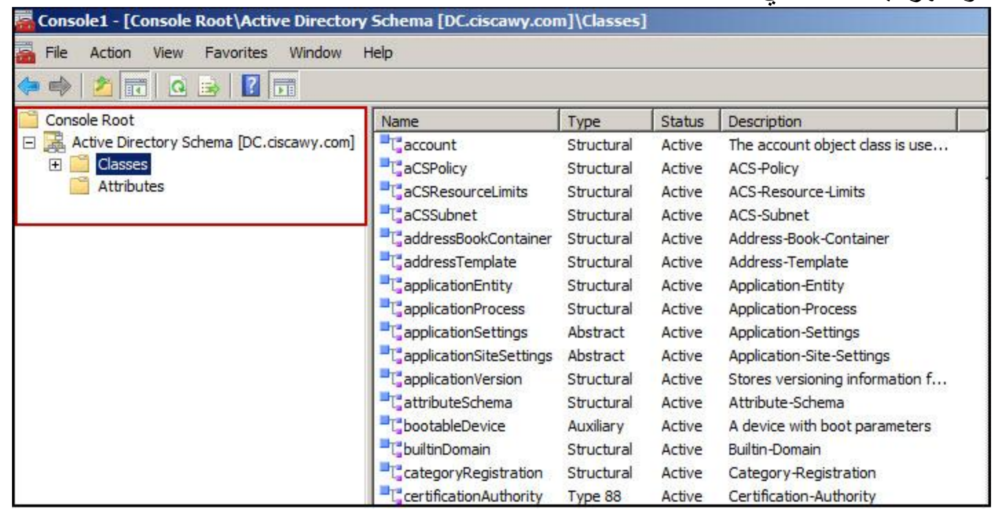
Start → run → MMC بعد كدا
File → add/remove snap in



ونختار الActive Directory Schema ونعمل add ثم OK

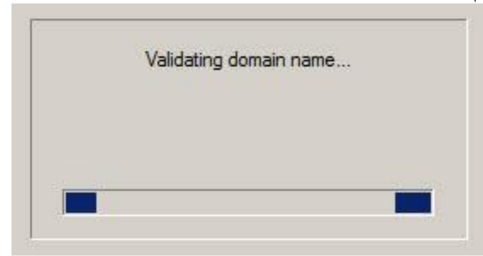


هتتفتح معانا وتظهر لينا القائمه دي



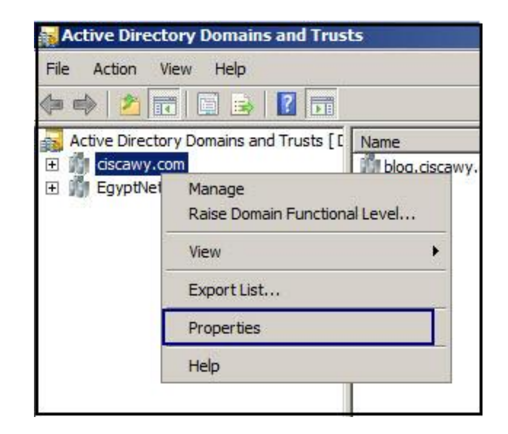
2- Domain Name Master

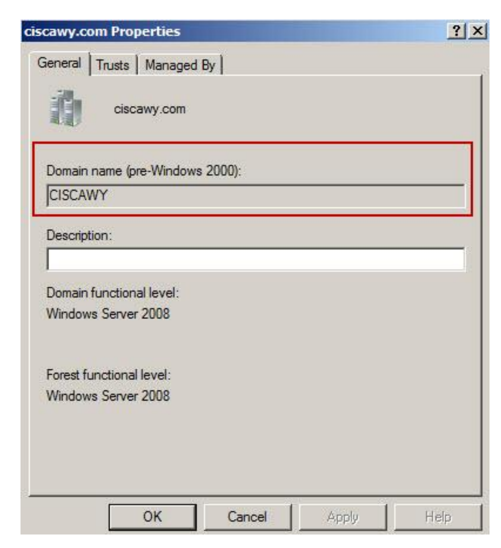
- نتذكر حينما نقوم بانشاء Domain جديد أيا كان نوعه ،، تجده انه يقوم بعمل process لبضع ثواني يقوم بالتأكد من ان هذا الأسم فريد Unique علي الForest
- حيث يجب الا يتكرر اسم الDomain



- لمعرفه مكان تخزين هذه الRole :-

من عن طريق الActive Directory Domain and Trust



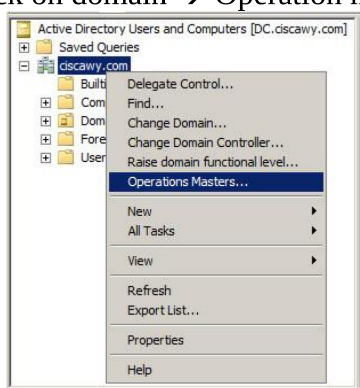


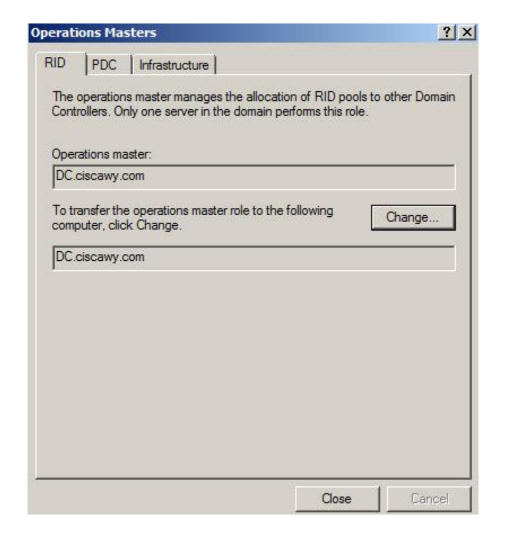
3- Relative Identifier Master (RID)

- مجموعه من الارقام علي شكل Pool تسمي الRID
- حينما نقوم بانشاء User او Computer كل منهما يكون له SID مختلف عن الاخر ويضاف له رقم يسمي RID من الPool
- تلاحظها حينما تقوم بعمل Migration لبعض المستخدمين من Domain لأخر حتي وان كانوا بنفس الاسم لا يحدث Replace لأنهم مختلفون في رقمي الSID و الRID
- لمعرفه مكان تخزين هذه الRole :-

Start ➔ administrative tools ➔active directory users and computers

R.click on domain → Operation master



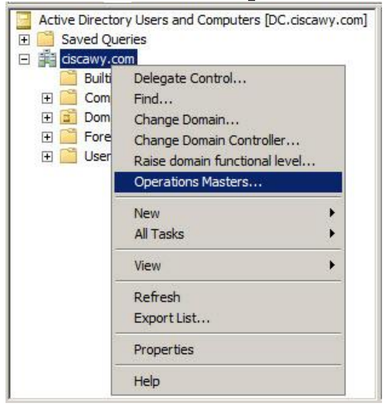


4-Primary Domain Controller Emulator (PDC)

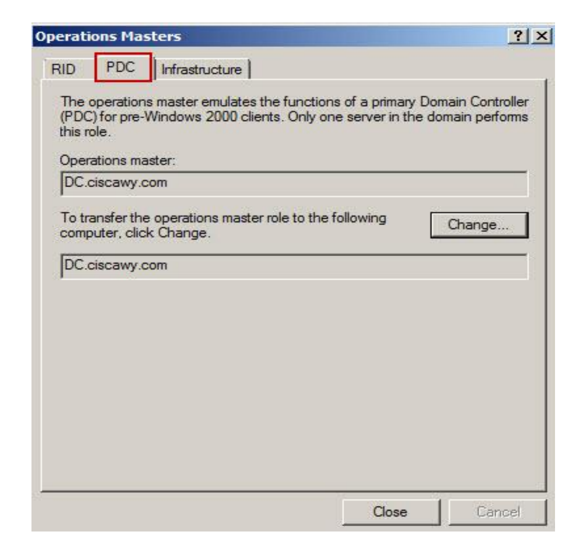
- بتحكم في الDate and Time
- Domain Master Browser المستعرض الاساسي للDomain
- يعالج التفاوت في كلمات المرور
- يعدل في الGroup Policy
- لو كنت بستخدم في الشركه الخاصه بي اي نسخه قديمه من ميكروسوفت يلعب الPDC Emulator دور الWindows NT PDC

- لمعرفه مكان تخزين هذه الRole :-

Start ➔ administrative tools ➔active directory users and computers
R.click on domain → Operation master



ونختار الPDC Tap

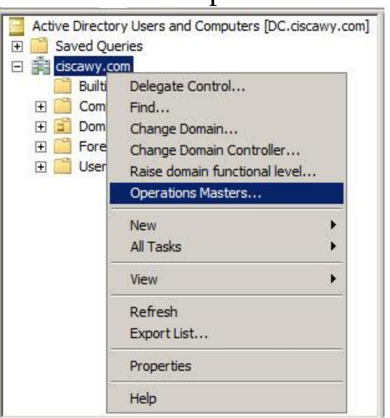


5- Infrastructure Master

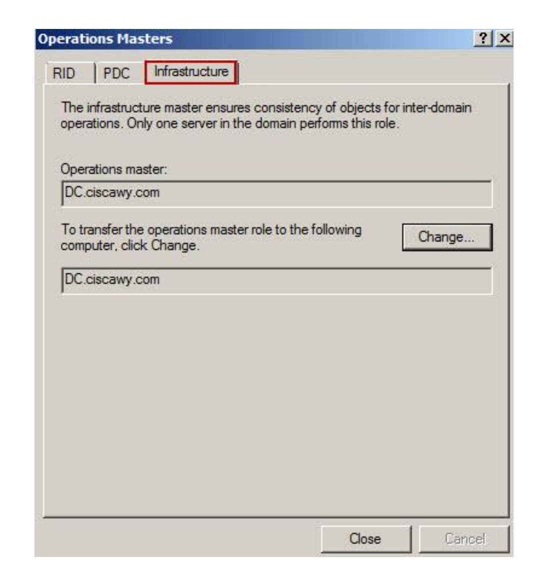
- خاصه بالبنيه التحتيه للDomain
- مسئوله عن responsible for updating references
- لمعرفه مكان تخزين هذه الRole :-

Start ➔ administrative tools ➔active directory users and computers

R.click on domain → Operation master



ونختار الInfra Tap



كيف نقوم بنقل Role من Domain لآخر !!!

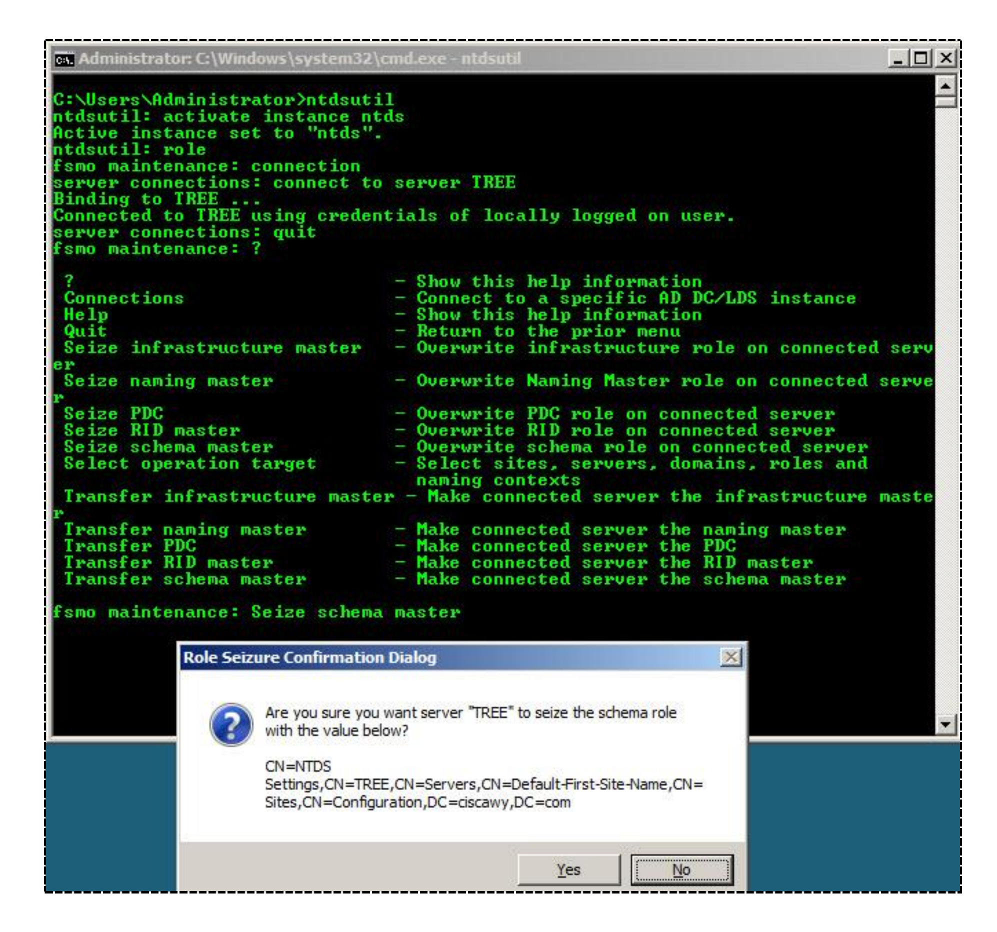
او بمعني اخر اني اقوم بنقل الSchema Role من Domain لأخر – اغير المالك لها –

Start ➔ run ➔ cmd

- ntdsutil
- activate instance ntds
- role
- connection
- connect to server (server name)
- quit
- ?

  عشان نشوف ايه ممكن نعمله من الاوامر دي

  اخرDomainأي اني يمكنني ان انقل اي منهم ل
- Seize schema master (مثال)



لمعرفه أماكن تخزين ال FSMO Roles

Start ➢ run ➢ cmd
dsquery server -hasfsmo schema
dsquery server -hasfsmo rid
dsquery server -hasfsmo pdc

علي الDomain الرئيسي بعدما نقلت الSchema Role سنجد انه تظهر رساله Error لأنني قمت بنقله

```
C:\Users\Administrator>dsquery server -hasfsmo schema
Error code = 0x8000500d
type dsquery /? for help.
C:\Users\Administrator>
```

واذا قمت بكتابه اي امر ثاني سينجح الامر

```
C:\Users\Administrator>dsquery server -hasfsmo rid
"CN=DC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=ciscaw
y,DC=com"
```

علي الNew Tree سنجد ان أمر الSchema فعال علي هذا الDomain

```
C:\Users\Administrator>dsquery server -hasfsmo schema
"CN=TREE,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=cisc
awy,DC=com"
```

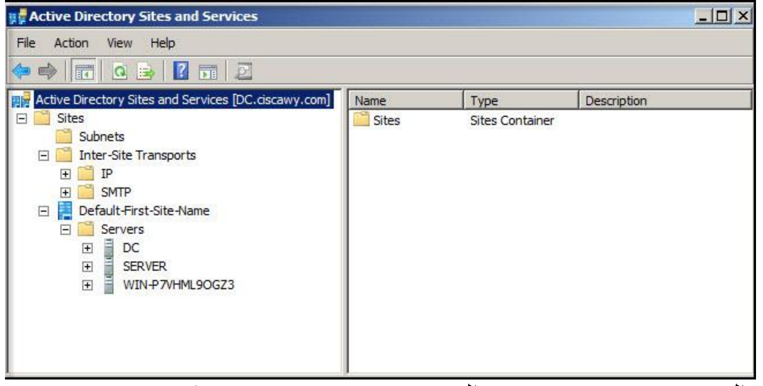
Active Directory Sites and Replications

- تتلخص فكره الSites and Replication هو ضمان حدوث التضاعف بين ال Domains
- احيانا لا تكون الAdditional , Child , Tree في نفس المكان او في نفس الموقع ويكون كل منهما في مكان مختلف ،،
- لذلك يتوجب عليا ضمان حدوث الReplication بينهما
- لهذا الغرض اقوم بوضع كل Domain او مجموعه Domains في Site link مختلف علي حسب موقعه الجغرافي واقوم بربطهما مع بعض
- بتتحكم في وقت المخصص للReplication وايضا لتقليل نسبه ال Load بين ال Domains
- ذكرنا من قبل انه حينما تقوم بانشاء اول Domain في ال Forest الخاصه بك يكون

By-default → Default first site name

- لكي اقوم بانشاء اي Domain في اي Site اخر يمكنني ان اقوم باعدادها من الاعدادت الاوليه و سنراها لاحقا
- للتعامل مع هذا ال Console

Start ➔ administrative tools ➔Active Directory Sites and Services



- سنجد هنا ان كل الServers موجوده تحت الDefault First Site Name
- طريقه إيصال ال Updates او طريقه عمل ال Replication بين الSites

اما عن طريق ال IP او عن طريق ال SMTP

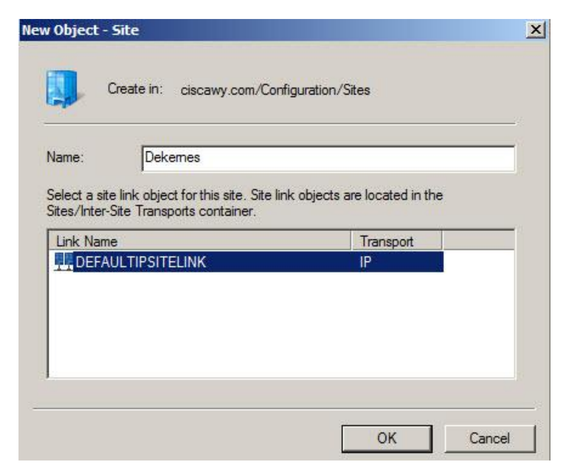
SMTP	IP
○ يستخدم بين ال Domains في نفس الSite ○ يرسل التحديثات عن طريق ارسال الE-Mails بين الDomains	○ يستخدم بين ال Domains في نفس الSite ○ او بين اكثر من Site ○ يقوم بإرسال Sen , Ack , sen ack للتأكد من اتمام الاتصال ○ يعتبر اسرع بكثير من الSMTP

- لأنشاء Site جديد R.click on Sites → New Site

Create additional sites when:

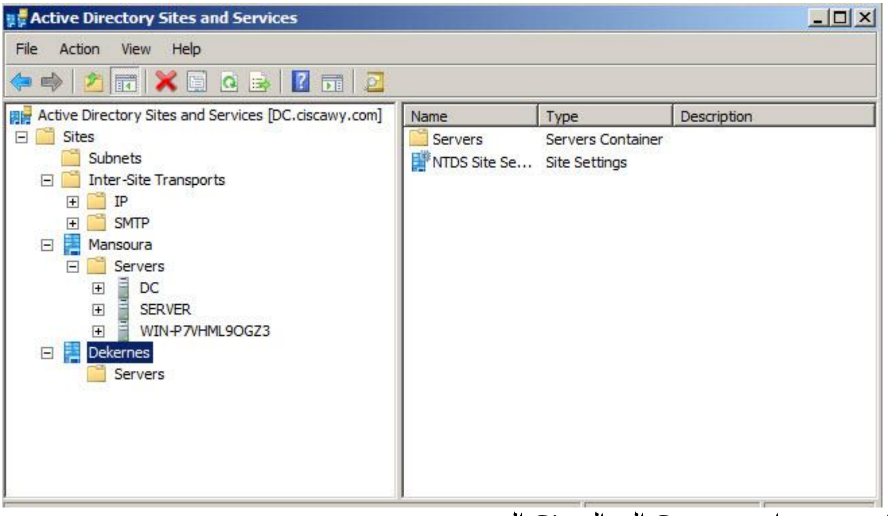
- A part of the network is separated by a slow link.
- A part of the network has enough users to warrant hosting domain controllers or other services in that location.
- Directory query traffic warrants a local domain controller.
- You want to control service localization.
- You want to control replication between domain controllers.



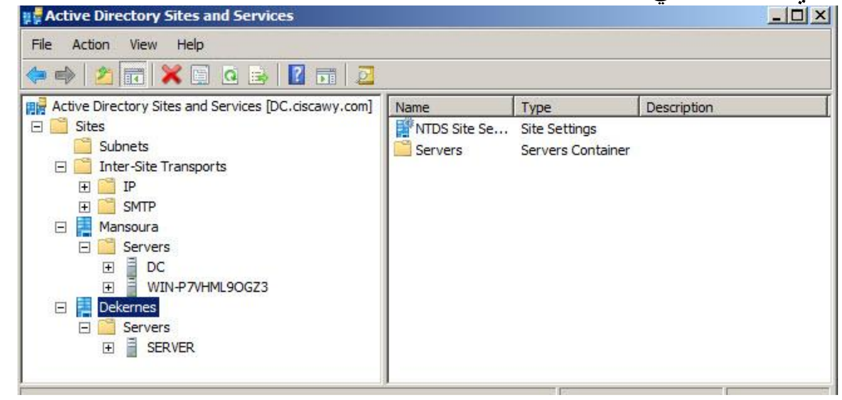


ثم نضغط علي Enter

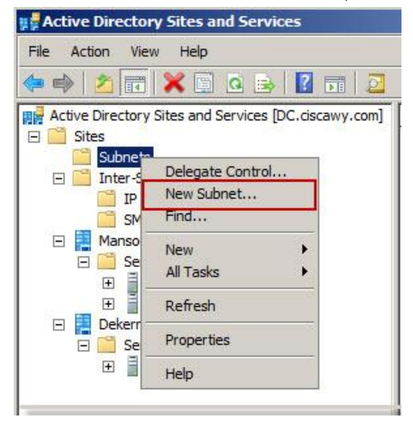
- قمت بإعاده تسميه الDefault first site name الي Mansoura
- ستجد ان تحت قائمه الSite الجديد Dekernes



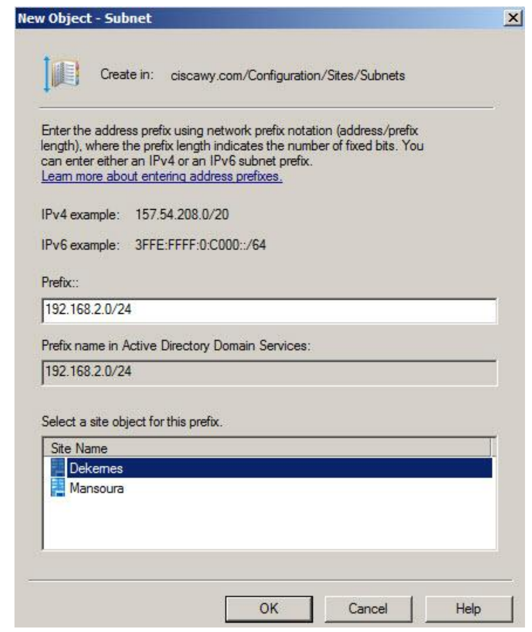
- نقوم بسحب اي Server الي الSite الجديد



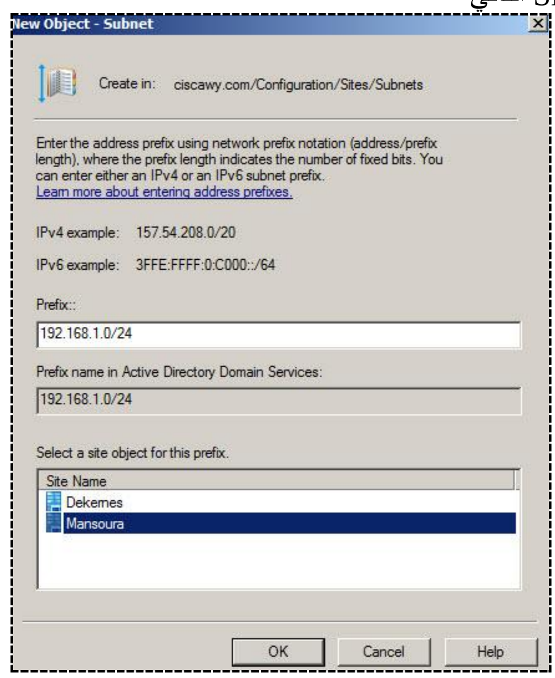
- لابد من ان نضيف Subnet الخاصه بالDomain لكل Site



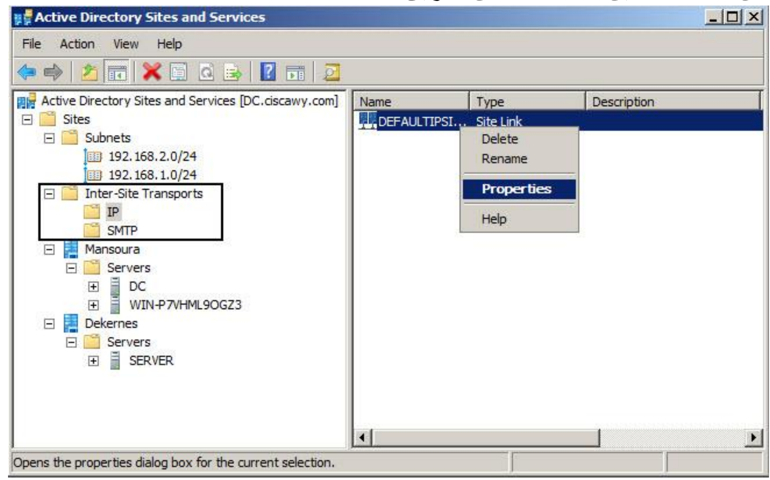
واضيف الSubnet لكل Site



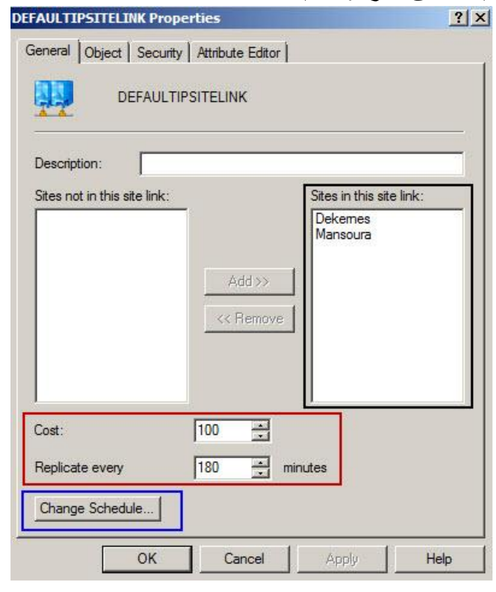
ونقوم بإنشاء Subnet لل Site التاني



- لتعديل خصائص الاتصال بين الSites عن طريق ال IP



سنجد بها بعض الخصائص التي يجب ان تدركها جيدا ،، !!



- Sites in the site link

- هنا بيوضحلك انهي Sites مربوطين مع بعض بالLink دا
- ممكن تضيف Link تاني او تزيل واحد قديم

- Cast

- تلقائيا تكون 100 يمكنك ان تزودها او تقللها ،،
- ويمكنك ايضا ان تنشأ Site link اخر بين نفس الTwo Sites وتقلل او تزود في الCast اذا كنت تريد احداهما الاول
- واذا تركت الCast في كلاهما 100 سيقوم بعمل Balance بين الTwo Links

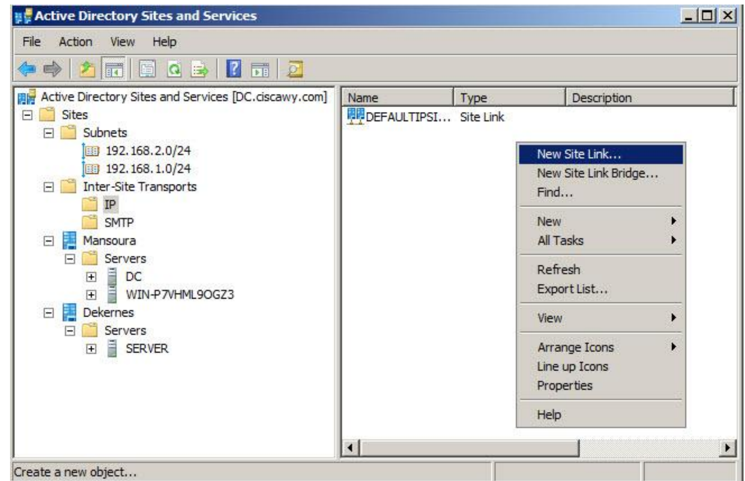
- Replication Every

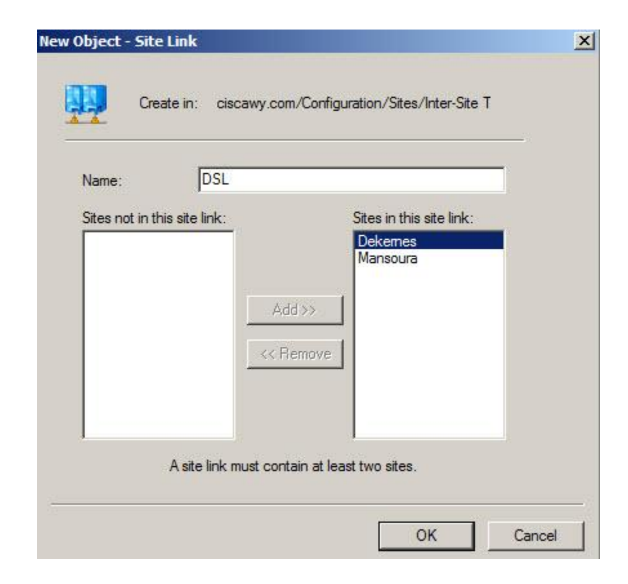
- اي وقت التضاعف بين الSites
- تلقائيا في نفس الSite تحدث في نفس ذات الوقت
- اما بين الDifferent Sites تكون كل 3 ساعات
- لابد ألا يقل عن 15 ،، ولا يقبل اي اوقات اخري سوا مضاعفتها أي 15 , 30 , 45

- Change Schedule

- من خلاله ممكن اعمل جدول معين لأوقات التضاعف في ايام محدده وساعات محدده ايضا

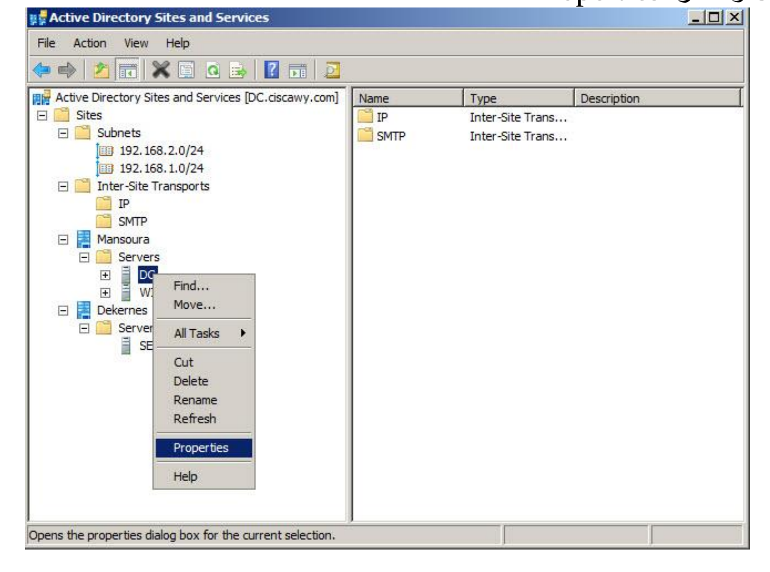
- لأنشاء Site Link جديد تربط نفس الSites

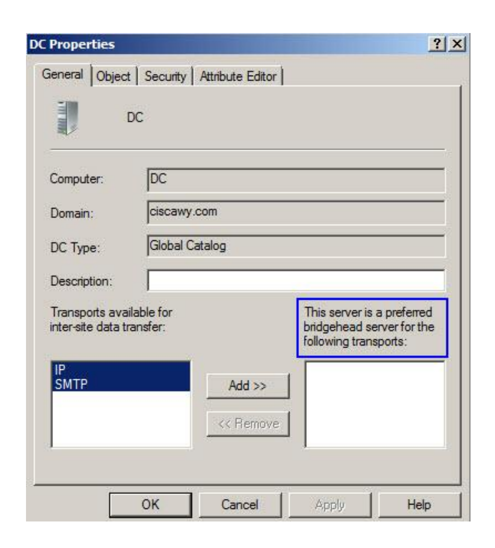




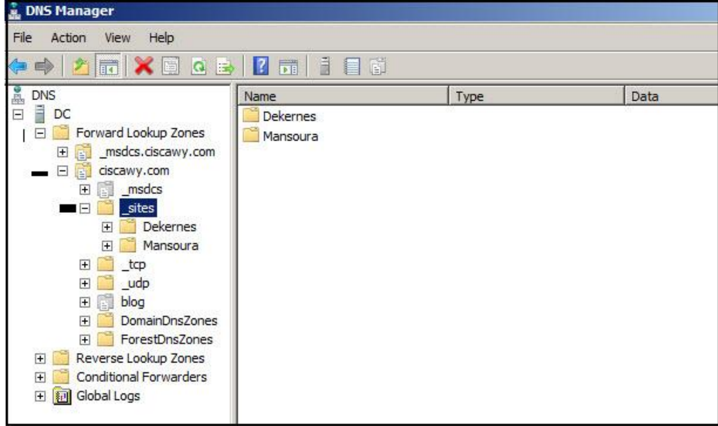
ثم نضغط علي OK
بعد ذلك يمكننا تغيير الCast والReplication time والSchedule

- الBridge Head
  - دا الDomain الرئيسي المسئول عن عمل الReplication الخارجيه في كل Site
  - وبختار نوع الReplication عن طريق ال IP أو الSMTP
  - R.click علي اي Server واختار Properties



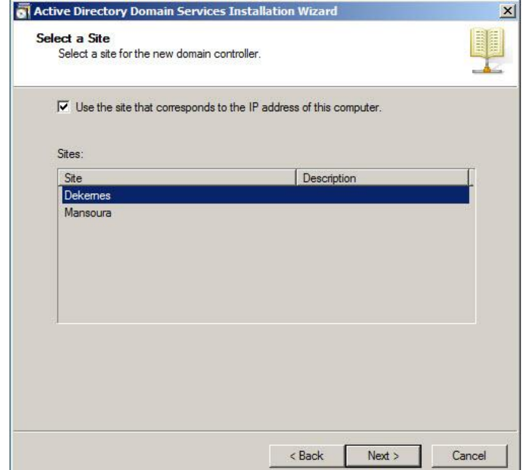


- للتأكد ايضا من انه تم انشاء Two Sites علي هذا الDomain :-
  نقوم بفتح ال DNS



وكل User علي حسب مكان Domain بتاعه فيSite سيقوموا بعمل ال Authentication

- قمت بأنشاء Domain Child سريعا بعد انشاء الSites لأوضح لك انه يمكنك ان تختار بعد ذلك اينما تريد ان تضع هذا الDomain وانت تجري عمليه ترقية الServer الي ان يكون Child Domain



- اذا رجعت للفصل الذي يتحدث عن كيفيه إنشاء الChild Domain ستجد ان هذه الصوره مختلفه كثيرا

Active Directory replication is:

- MultiMate replication
- Pull replication
- Store-and-forward

- Partitioning of the data
- Automatic
- Attribute-level replication
- Distinct control of intra site replication
- Collision detection and management

Replication Transport Protocols

- **Directory Service remote Procedure call (DS-rPc) DS-RPC** appears in the Active Directory Sites And Services snap-in as IP. IP is used for all intrasite replication and is the default, and preferred, protocol for intersite replication.
- **Inter-Site messaging—Simple mail transport Protocol (iSm-SmtP)** Also known simply as SMTP, this protocol is used only when network connections between sites are unreliable or are not always available.

The Intersite Topology Generator (ISTG) creates connection objects between Bridgehead servers that share a site link

Within a site, domain controllers replicate quickly, using a topology generated by the Knowledge Consistency Checker (KCC), which is adjusted dynamically to ensure effective intersite replication

Replication :-
Intra Site → Every 15 Second with 3S for Delay
Inter Site → Evert 3 Hours

Trust

- الثقه المتبادله بين الانواع المختلفه من الDomains
- لها نوعان :
  - Two Way اي ان كلاهما يمكنه ان يتحكم في الاخر.
  - One Way لأحدهما خاصيه التحكم في الاخر علي حسب ما تم من اعدادات لهذا الموضوع
- البروتوكول المسئول عن عمليات الوثوقيه بين الDomains يسمي
Kerberos Authentication Protocol

- Parent and Child
Default two ways in the same forest

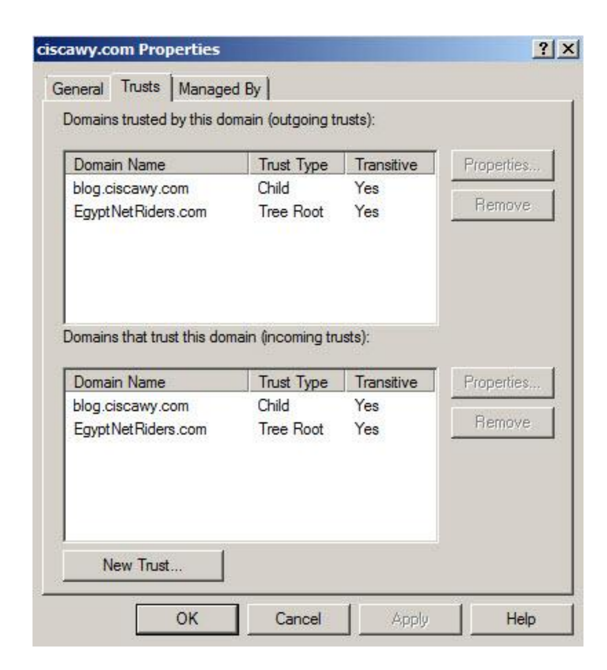
- Tree Root
Default two ways
Between Tree root domain and other Tree root domain

- Shortcut Trust
One or Two way
Between Child in Tree and Child in other Tree

- External Trust
One or Two way
Between any Domain in Forest and any other Domain in other Forest
Trust not inheriting لا تتوارث

- Forest Trust
One or Two way
Between Forest Root Domain in Forest and other Forest Root Domain in other Forest

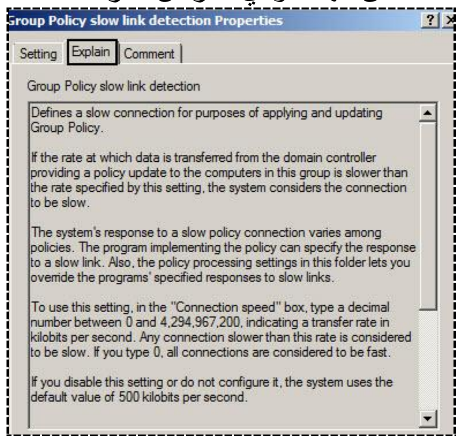
- Realm Trust
One or Two way
Between Microsoft Operating System and other Operating System likes Linux



صوره من الTrast المنشأة تلقائيا في نفس الForset
حينما نقوم بعمل Child Domain او New Tree

Group Policy

- مجموعة من السياسات ، التعقيدات ، ال Restrictions التي نقوم بتطبيقها علي المستخدمين
- تطبق ال Policy علي مستوي الOU , Sites , Domain فقط ولا تطبق علي الGroups
  Start ➔ administrative tools ➔ Group policy management
- اهميه الPolicy لا تتوقف فقط علي اجراء التعقيدات علي المستخدمين ، بل ايضا يمكن من خلالها نقوم بتنصيب اي برامج يحتاجها المستخدمين Deploy Software
- يفضل حينما تقوم بإنشاء Policy جديده ان تسميها علي حسب الغرض التي ستؤديه حتي يسهل عليك بعد ذلك متابعتها وتصحيح الاخطاء
- لا توجد قواعد محددة في الPolicy ولكن علي حسب ما يطلب منك تقوم بالبحث في الPolicies عما يؤدي لهذا الغرض
- لكل Policy شرح ويمكنك قراءته للتأكد من انها ستؤدي الغرض المراد



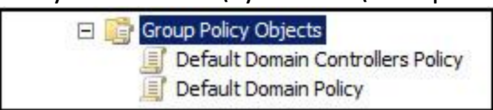
- ايضا من خلالها يمكننا منع اي مستخدم من انه يتحكم في اي مكون من مكونات الجهاز اي نتحكم في غلق منافذ الUSB وايضا في ال DVD Rom
- من خلال الPolicy ايضا يمكننا ان نتحكم في مواعيد دخول المستخدمين علي الأجهزه
- يمكن ايضا ان نقوم بغلق كل الApplications علي المستخدمين ونترك فقط برنامج معين
- تطبق الPolicy علي مستويين User and Computer Account

USER ACCOUNT	COMPUTER ACCOUNT
▪ تطبق الPolicy عند الLog on ▪ Assign and Publish Software	▪ تطبق الPolicy عند الStart Up ▪ Assign Software فقط

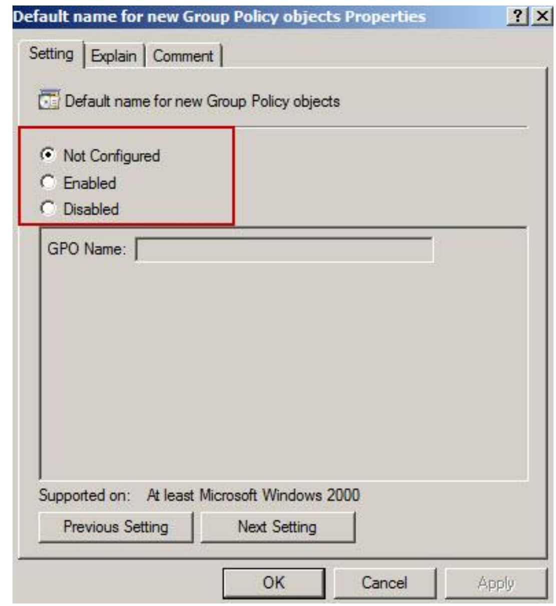
- تلقائيا يكون هنا Two Applied Policies احداهما
  علي مستوي الDomain Controller ويتم التحكم من خلالها في المستخدمين
  والاخري Local Domain Policy

مكان حفظ الـ Local GPOs

%SystemRoot%\System32\GroupPolicy

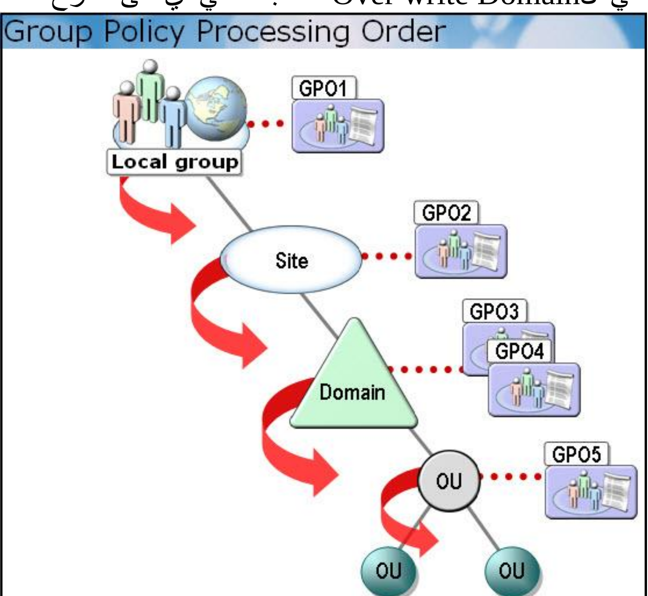


- للPolicy ثلاث انواع Not configured , Enabled , Disabled
  وعلي حسب الPolicy تختار نوعها

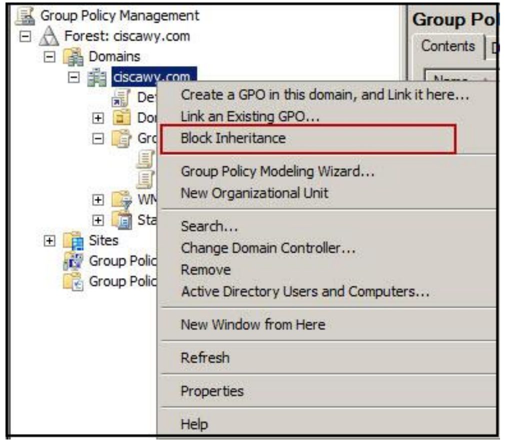


- تحدث عملية توارث للpolicy من علي الDomain ثم علي الSite ثم علي الOU

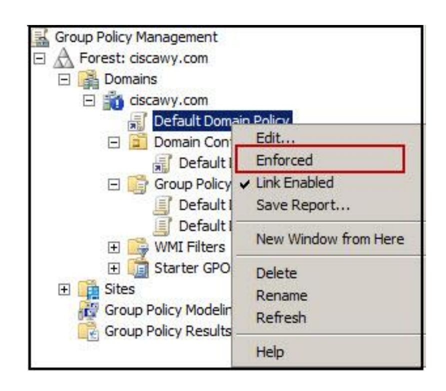
أي ان الPolicy المطبقه علي الDomain Over write المطبقه علي اي شئ متفرع منه



- اذا حدث اي تعارض بقوم بوقف علميه التوارث Block Inheritance
- ستجد ان علي الDomain علامه تعجب زرقاء !



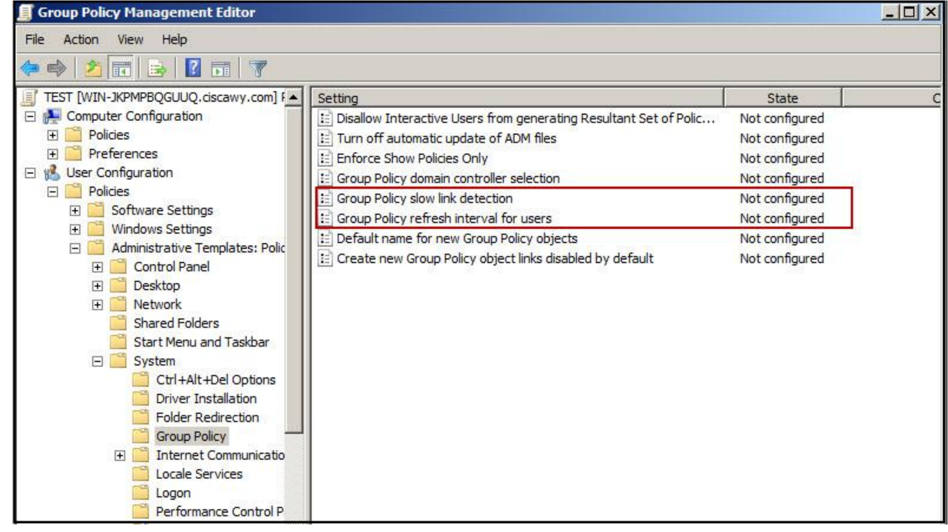
- لو تم منع التوارث بين الObject و هناك Policy اريد ان اطبقها بشئ اساسي او اطبقها علي كل المستخدمين Enforced



- كل ٩٠ دقيقه يقوم الServer يعمل تحديث لكل الPolicies ولكننا يمكننا ان نتحكم في هذا الوقت
- لتفعيل الGroup Policy يتم كتابه امر gpupdate في الCmd → Run → Start

واذا حدثت اي مشاكل او لم ينجح الامر يتم كتابه امر gpupdate /force حتي يتم تنفيز ها بالقوه
علي مستوي الUser او الComputer نقوم بفتح

Policies → administrative template → system → group policy



Refresh Interval دي المسئوله عن الوقت الخاص بتحديثات الPolicy ويمكنك التعديل في الوقت علي حسب رغبتك او سياسات الشركه

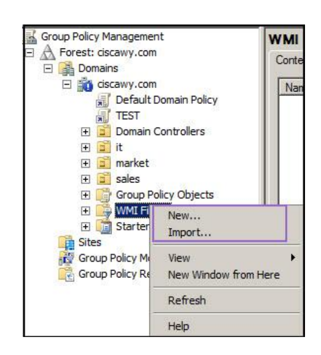
Slow link detection علي حسب سرعه الانترنت الموجود عندك وهي تلقائيا تكون 500kb/ps يمكنك ان تزودها علي حسب رغبتك

- WMI Filter

- بعض الفلاتر تلقائيا يتم وضعها في ال Policy وتطبيقها علي الUser
- يمكن نسخها او عمل لها Import
- تستخدم ايضا في عملية المراقبه والTroublshooting

- Windows Management Instrumentation (WMI) is a management infrastructure technology that allows administrators to monitor and control managed objects in the network.
- A WMI query is capable of filtering systems based on characteristics, including RAM, processor speed, disk capacity, IP address; operating system version and service pack level, installed applications, and printer properties.
- Because WMI exposes almost every property of every object within a computer, the list of attributes that can be used in a WMI query is virtually unlimited.
- WMI queries are written using WMI Query Language (WQL).

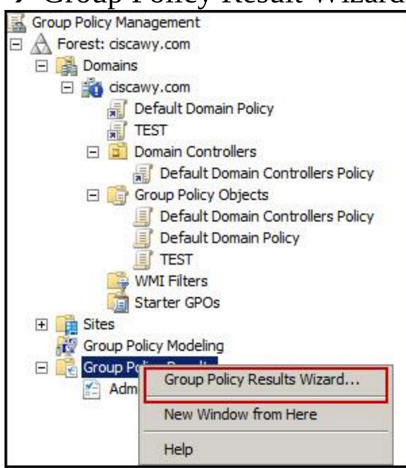
R.click on WMI filter → New



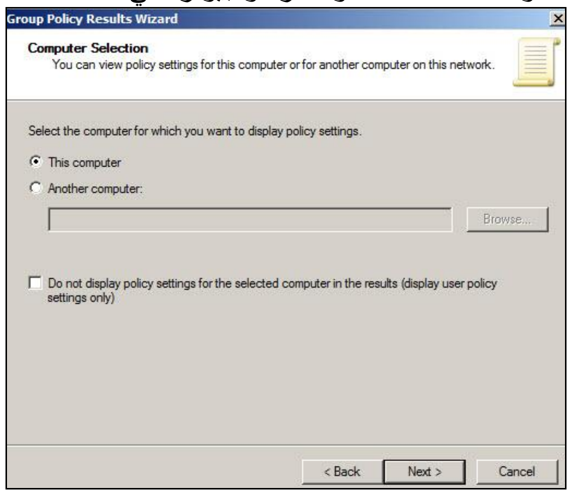
- Group Policy Result

- بشوف فيها الPolicy المطبقة علي ال Computer Account سواء اللي عليه الDC او اي جهاز تاني

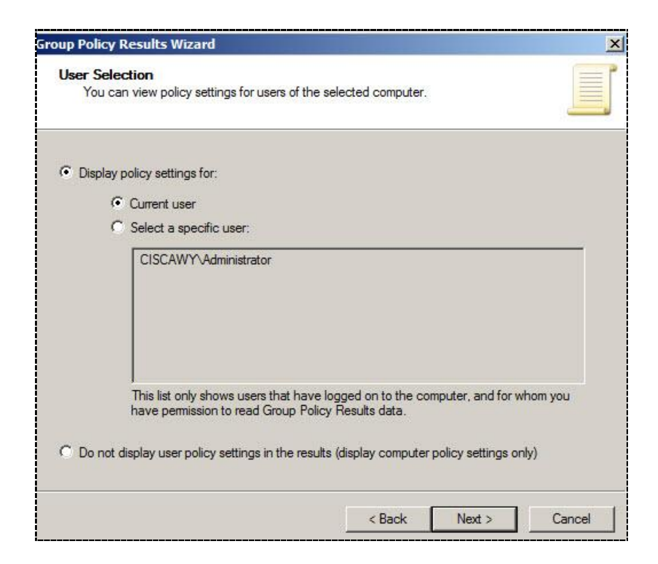
R.click → Group Policy Result Wizard → Next



ممكن اختار سواء الكومبيوتر دا او اعمل Browse واختار كومبيوتر تاني



ممكن اختار برضه من هنا ال User اللي بيعمل Logon علي الMachine دي



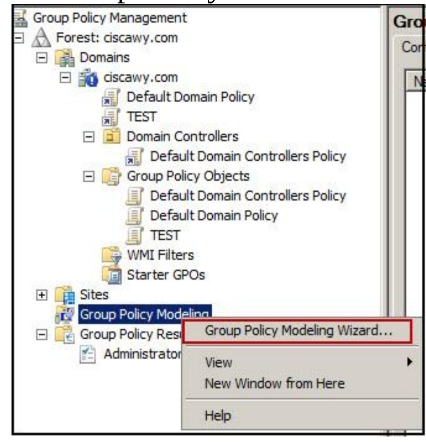
Next → Next → Finish

هيظهر ليك علي اليمين كل الPolicies اللي انت مطبقها

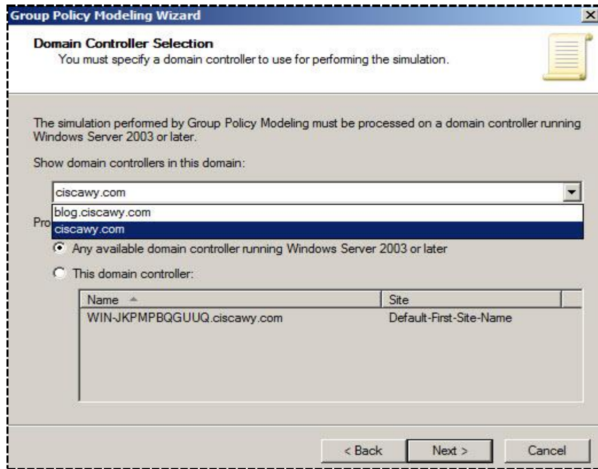
- Group Policy Modeling

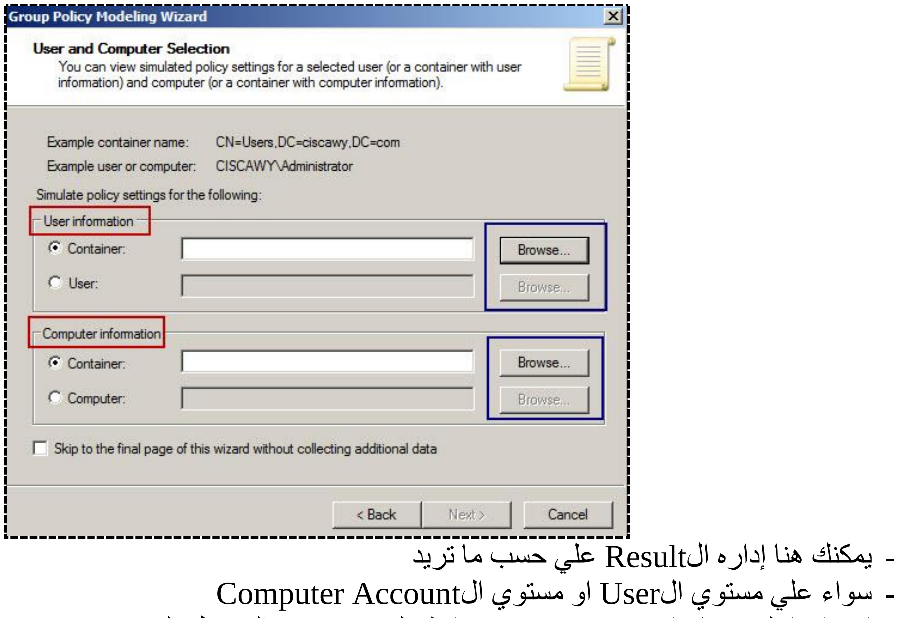
- نفس فكره الGroup Policy Result ولكن من خلالها يكون هناك خيارات اكتر
- الغرض الاساسي منها هو عمليه مراقبه او متابعه او Troubleshoot للPolicies اللي انا مطبقها علي مستوي الForest حتي تسهل عمليه الاداره والمراقبه ،، لتجنب حدوث اي مشاكل
- ممكن من خلالها معرفه الPolicies اللي علي Domains معايا في نفس الForest
- ايضا ممكن معرفه الPolicies اللي علي الSites والOU

R.click → Group Policy Result Wizard → Next

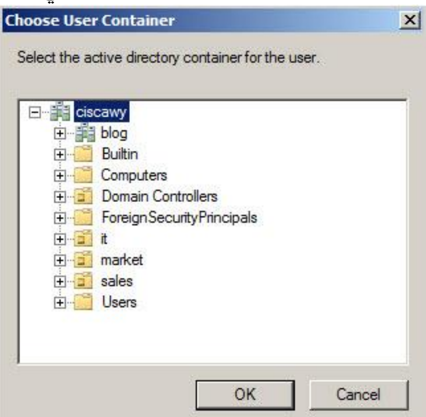


من هنا ممكن تختار اي Domain



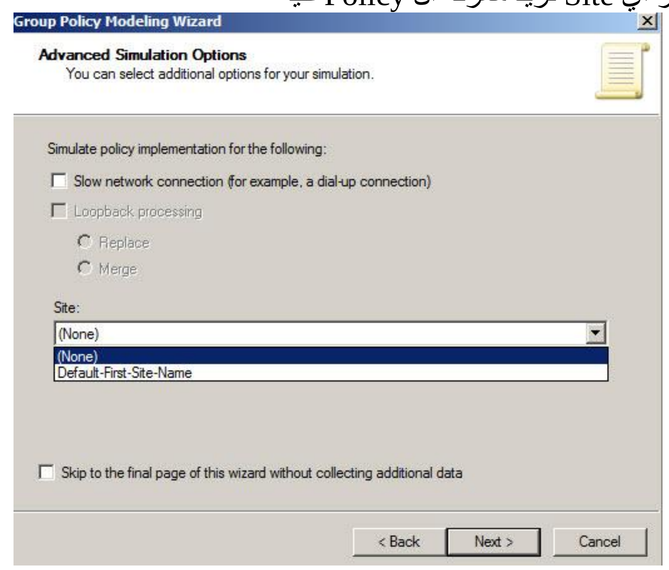


- يمكنك هنا إداره الResult علي حسب ما تريد
- سواء علي مستوي الUser او مستوي الComputer Account
- ايضا يمكنك اختيار اي Container من داخل الDomain بالضغط علي Browse وتختار اللي انت عايزه



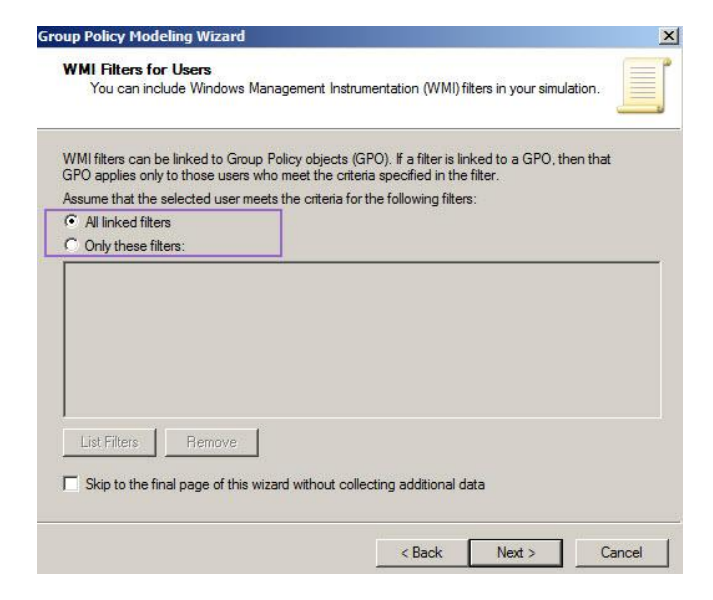
بعد كدا Next

- يمكنك ايضا اختيار اي Site تريد معرفه ال Policyعليه



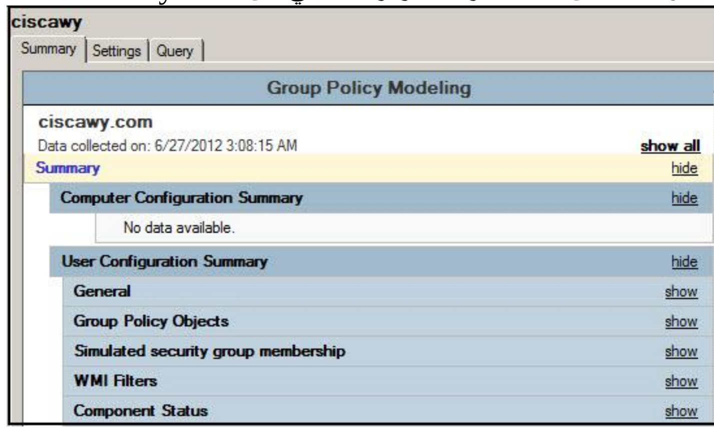
بعد كدا Next

- ممكن نختار ايضا علي حسب الFilter لو تم وضعه من قبل



Next → Next → Finish

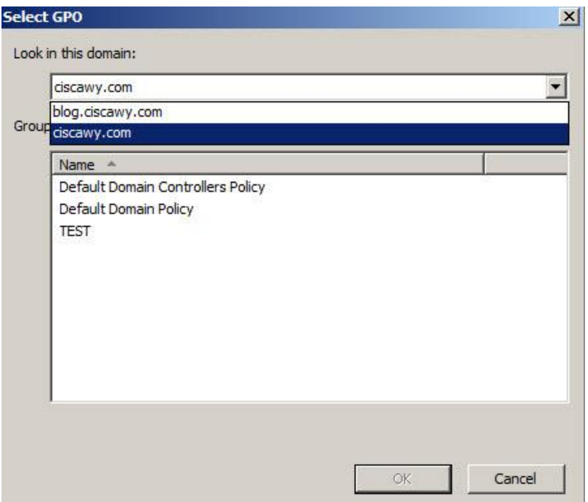
وهذه هي الصوره النهائيه ويمكنك من خلالها قراءه تقرير تفصيلي عن هذه الPolicy



- يمكنك ان تقوم بتعديل في Policy او تنشأ واحده جديده ثم تقوم بربطها بالOU التي تريدها

R.click علي الOU ثم اختار



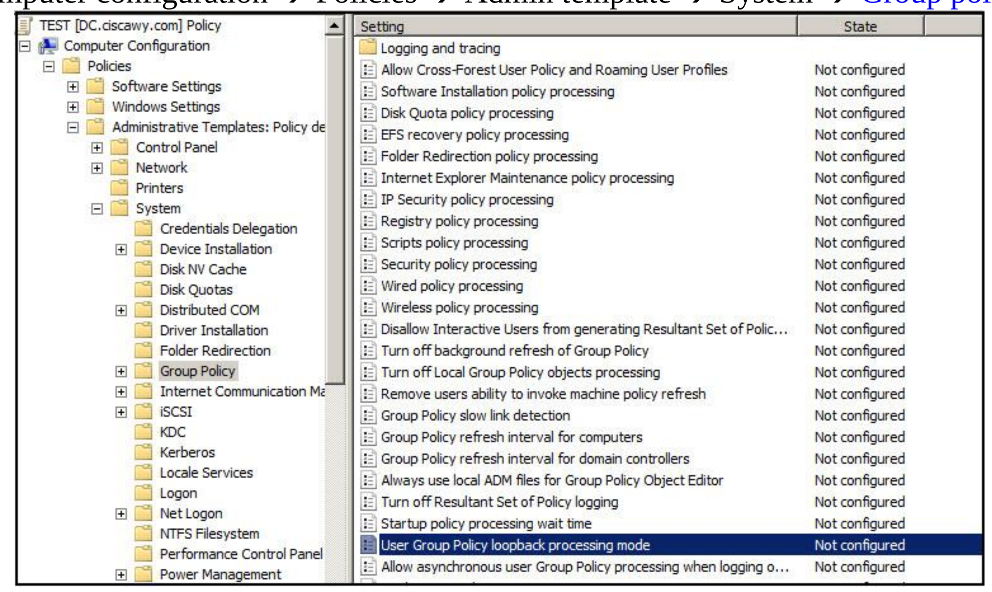


وتختار من هنا الPolicy سواء كانت موجوده علي ال Domain دا او علي Domain تاني في نفس الForest

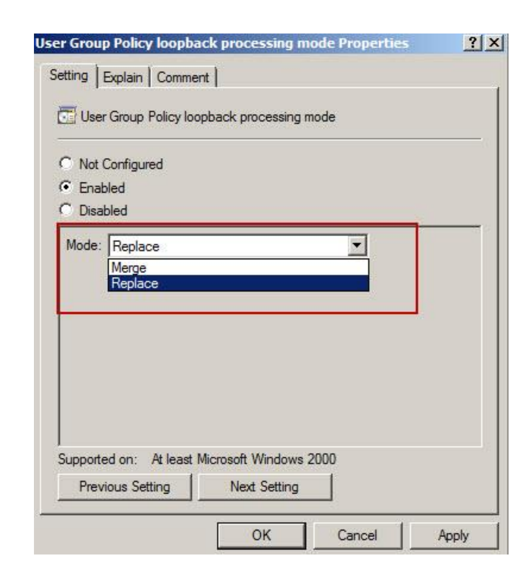
- إذا كان لديك مستخدم له صلاحيات في ان يدخل علي اكثر من Domain وكانت الPolicies المطبقه علي كلاهما متضاربه

في هذه الحاله هناك Policy تسمي Loop Back Process تطبقها علي هذا المستخدم

Computer configuration → Policies → Admin template → System → Group policy



ليها Two Modes
Replace ← هيطبق الPolicy الخاصه بالDomain اللي المستخدم عليه
Merge ← سيتم عمل دمج للاثنين،، لزياده الRestriction علي المستخدم



- Deploy Software

كإحدي أغراض الGroup policy هي ان يتم تطبيق او تنصيب تطبيقات او برامج علي كل المستخدمين في نفس الوقت

TABLE 7-1 Software Deployment Options

	PUBLISH (USER ONLY)	ASSIGN (USER)	ASSIGN (COMPUTER)
After deployment of the GPO, the software is available for installation:	The next time a user logs on.	The next time a user logs on.	The next time the computer starts.
Typically, the user installs the software from:	Control Panel Add Or Remove Programs (Windows XP) or Programs And Features (Windows Server 2008, Windows Vista, and later).	The Start menu or a desktop shortcut. An application can also be configured to install automatically at logon.	The software is installed automatically when the computer starts.
If the software is not installed and the user opens a file associated with the software, does the software install?	Yes (if auto-install is enabled).	Yes.	Does not apply; the software is already installed.
Can the user remove the software by using Control Panel?	Yes, and the user can choose to install it again from Control Panel.	Yes, and the software is available for installation again from the Start menu, shortcuts, or file associations.	No. Only a local administrator can remove the software; a user can run a repair on the software.
Supported installation files:	Windows Installer packages (.msi files) and .zap files.	Windows Installer packages (.msi files).	Windows Installer packages (.msi files).

- Software Distribution Point

النقطه المركزيه الموجوده علي الشبكه الداخليه التي عن طريقها يحدد الPath الخاص بالبرنامج

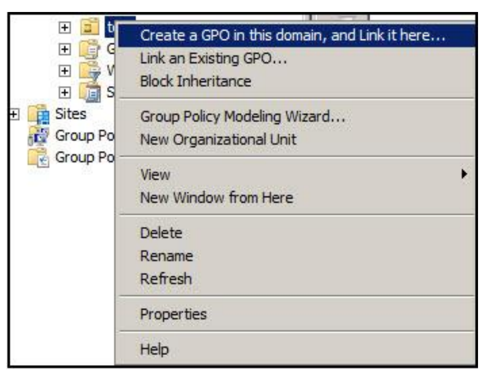
- بعض الملاحظات الهامه :-

  - يجب ان يكون امتداد البرنامج الExtension ان يكون .msi او .zap
  - يجب ان يتم وضع البرنامج في Shared folder
  - يسمي التطبيق او البرنامج بالPackage
  - نفس المسار علي أين من حساب الUser و الComputer

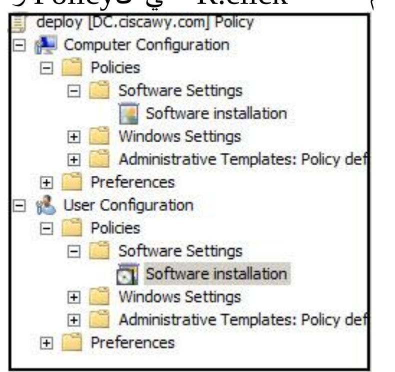
- أنواع الDeploying

Assign	**Publish**
• يستخدم علي حساب كل من الUser والComputer • في هذا الاختيار يكون التطبيق تم تنصيبه علي أين منهما و لا يتدخل أحد في اتمام عمليه التنصيب	• **يستخدم فقط علي الUser Account** • **له نوعان :-** **Full 🡐 لا يتدخل المستخدم في عمليه التنصيب** **Partial 🡐 يتدخل المستجدم لأكمال عمليه التنصيب**

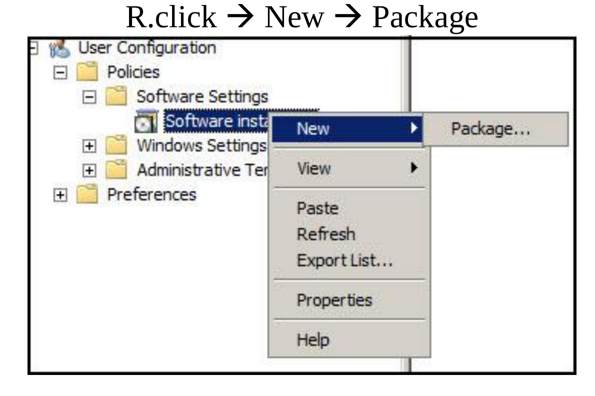
○ قمت بإنشاء OU سميتها Test ووضعت بها مستخدم له نفس الاسم
R.click علي الOU



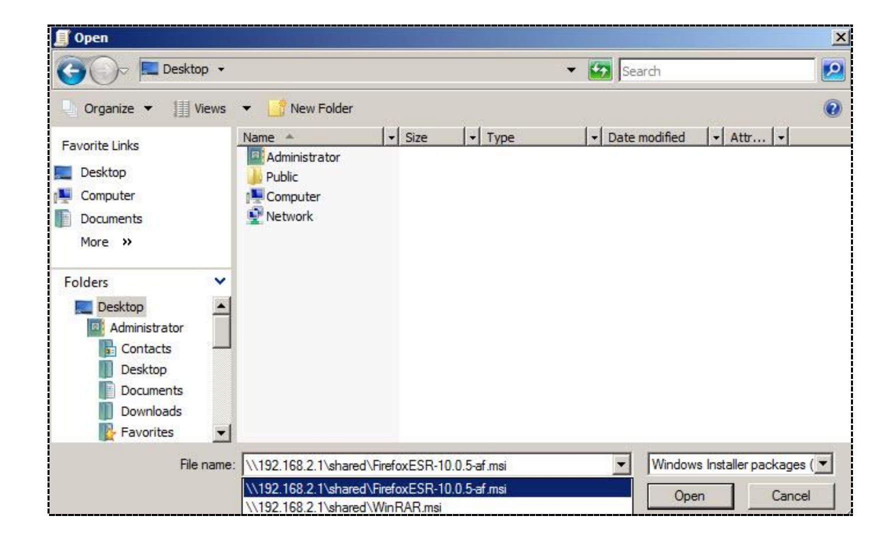
○ ثم نضغط R.click علي الPolicy ونختار Edit



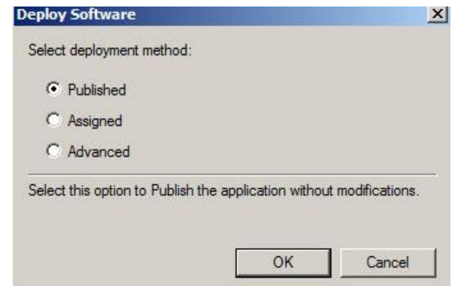
○ لنختبرها علي الUser Account
Policies 🡒🡒 Software Setting 🡒🡒 Software Installation
R.click 🡒 New 🡒 Package



○ ونختار مسار الShared Folder الموجود فيه ال Package



- وستظهر لنا هذه الاختيارات



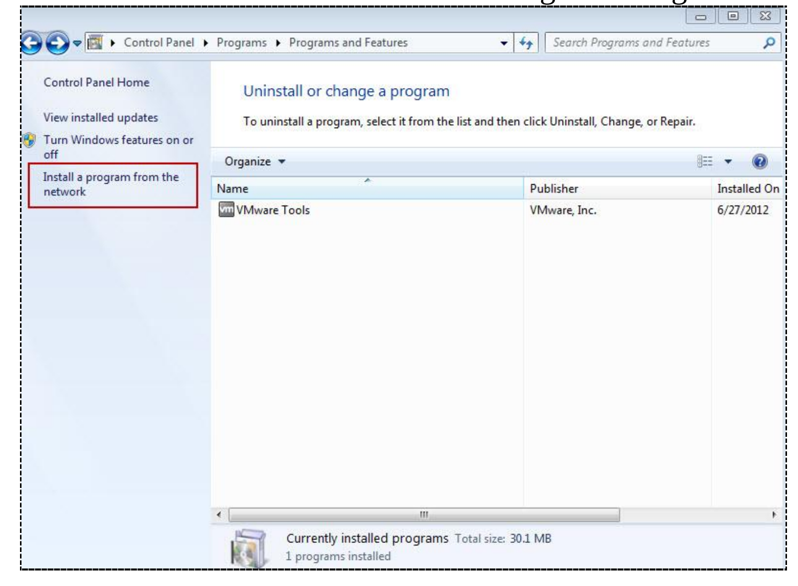
- اما عن Advanced فهي خاصه بالمخولين بعمليات الDeveloping في الشركه كتحديث بعض البرامج او اضافه اكواد جديده لها ولا تهمنا نحن كمديرين للنظام
- نختار Publish
- ثم نقوم بكتابه امر gpupdate /force في الRun

```
Updating Policy...
User Policy update has completed successfully.
```

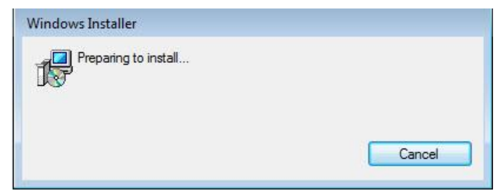
- علي جهاز ويندوز 7

نقوم بالدخول بحساب المستخدم الموضوع في الOU المطبق عليها هذه الPolicy

نقوم بفتح Control Panel\Programs\Programs and Features



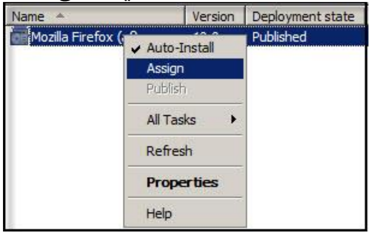
سيظهر لنا البرنامج ونقوم بالضغط R.click عليه ونختار Install



ستظهر لنا هذه الشاشه وتبدأ عمليه التنصيب



يمكن ان تغير من طريقه الDeploy عن طريق الضغط R.click علي الPackage وتختار النوع الآخر

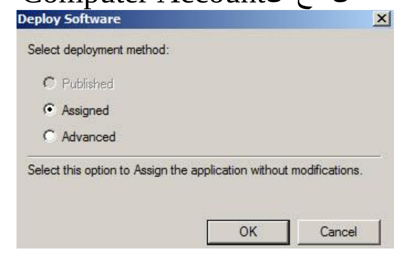


- علي الComputer Account

Policies ➔➔ Software Setting ➔➔Software Installation

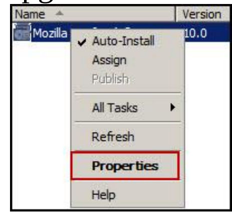
R.click → New → Package

ستجد ان الPublish ليست فعاله لأنها لا تعمل مع الComputer Account

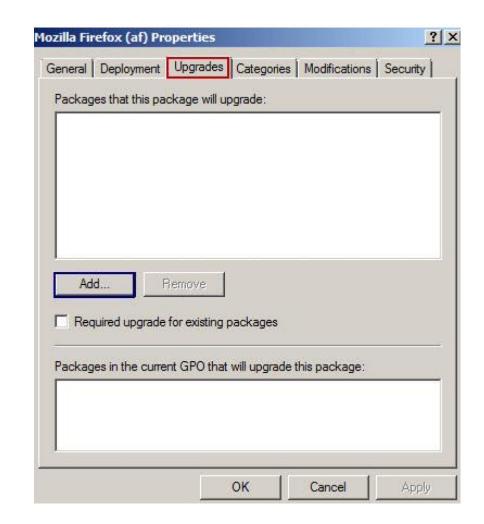


- بخصوص ما تم ذكره عن الAdvanced :-

R.click علي الPackage وتختار Properties ونختار الUpgrade

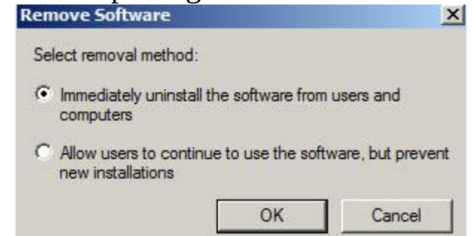


ونقوم بالضغط علي Add ونضيف الUpgrade الخاص بالSoftware وكما نوهت انها خاصه بالمبرمجين فقط



لحزف الPolicy الخاصه بعمليه الDeploying ،، هناك اختياران

R.click on package → all tasks → remove



بالنسبة للأول :- يتم مسح ال Policy ويحذف البرنامج من علي حساب كل من ال Userو الComputer

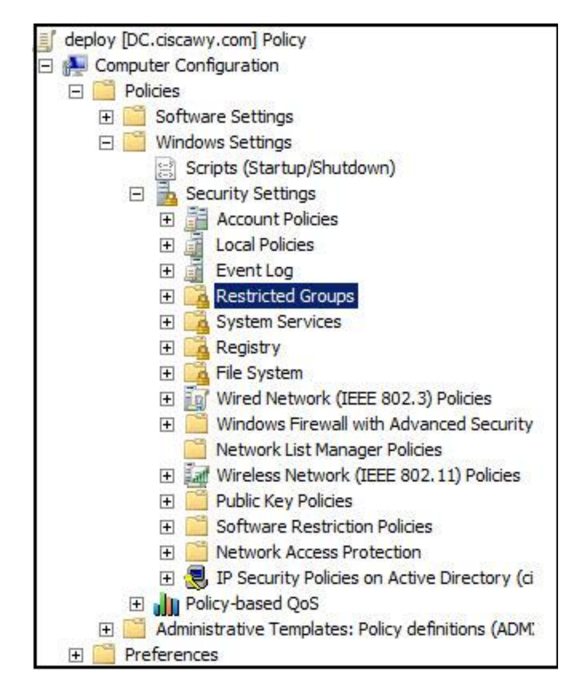
أما الثاني :- تمسح الPolicy فقط ويترك البرنامج علي المستخدمين ولكن لا يتم تنصيبه علي المستخدمين الجدد

- Restricted Groups

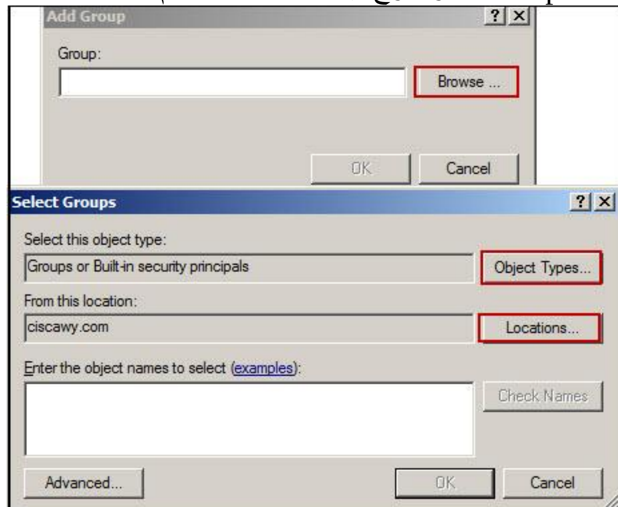
- لو انا مطبق Policy علي OU محدده ،، ولكن هناك مستخدم معين تم ترقيه الي مرتبة أعلي او اريد أن اعطيه بعض Features أخري
- أو أريد ان الغي من عليه هذه الPolicy
- يتم وضع المستخدم في Group و اضافته فيما يسمي الRestricted groups

Computer Configuration → Policies → Windows Setting → Security Setting → Restriction Groups

ثم نقوم بعمل Add Group → R.click



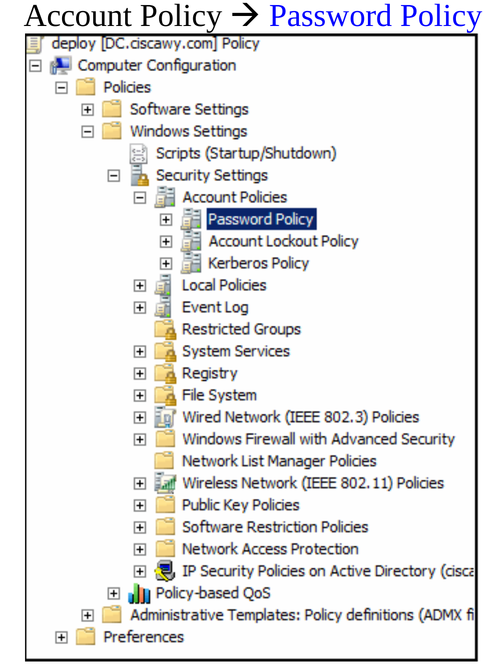
نضغط علي Browse ونضيف الGroup الموضوع فيها حساب المستخدم



Security in Group Policy

من احدي المهام الاساسيه للGroup Policy هي تطبيق بعض اساليب الحمايه علي المستخدمين
اساليب الحمايه متعدده بدايه من كلمات المرور.. التحكم في اوقات الدخول والخروج .. التحكم في Icons سطح المكتب ..
التحكم في كل ما يمكن ان يستخدمه الUser
وستتحدث عن بعضهما في هذا الفصل

Computer Configuration → Policies → Windows Setting → Security Setting
Account Policy → Password Policy

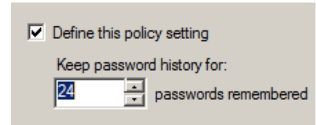


الخاصه بالPassword

Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Password must meet complexity requirements	Not Defined
Store passwords using reversible encryption	Not Defined

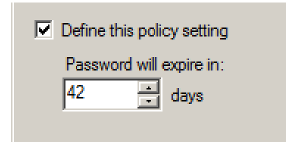
- :Enforce password history

حينما اقوم بتغيير كلمه المرور تقوم هذه الPolicy بمنع استخدام اخر عدد معين يتم تحديده من هذه الPolicy من كلمات المرور
يمكن ان اقوم بمنع استخدام اخر ٥ او ٧ كلمات مرور تم استخدامها من قبل هذا المستخدم
تلقائيا يتم منع اخر ٢٤ كلمه مرور تم استخدامها



-: Maximum password age

عمر او مده بقاء كلمه المرور صالحه أو العمر افتراضي لكلمه المرور
يفترض ان يتم تغييرها كل ٤٢ يوم ويمكنك ان تزيد هذه الفتره او تنقصها علي حسب سياسات الشركه

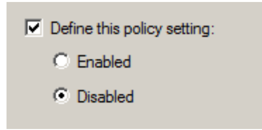


-: Minimum password age

أقل عمر افتراضي لكلمه المرور وهو لا يقل عن يوم وتتراوح من يوم الي ٩٩٨ يوم

-: Password must meet complexity requirements

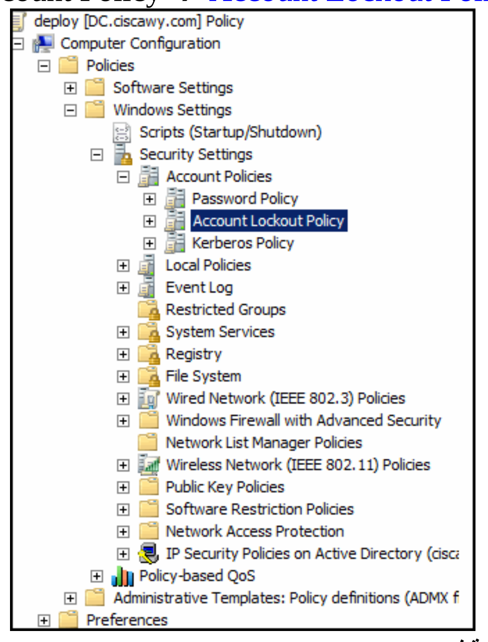
يجب ان تكون كلمه المرور معقده حتي يصعب كسرها واختراقها
كما نوهنا في بدايه الكتاب



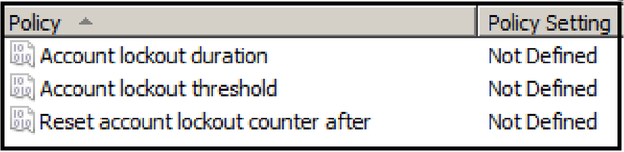
-: Store passwords using reversible encryption

خاصه بتشفير كلمه المرور
ويستخدم هذا البروتوكول في التشفير (Challenge-Handshake Authentication Protocol (CHAP

Computer Configuration → Policies → Windows Setting → Security Setting
Account Policy → Account Lockout Policy



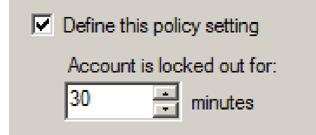
خاصه بأوقات دخول وخروج المستخدمين



Policy	Policy Setting
Account lockout duration	Not Defined
Account lockout threshold	Not Defined
Reset account lockout counter after	Not Defined

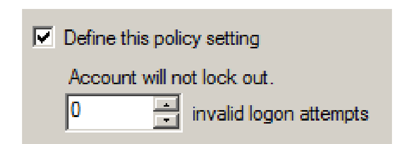
-: Account lockout duration

بعد كتابه كلمه المرور خطأ يتم غلق الحساب لفتره By-default 30 دقيقه
وبعدها يشترط ان يتم فتح الحساب من قبل الAdministrator



-: Account lockout threshold

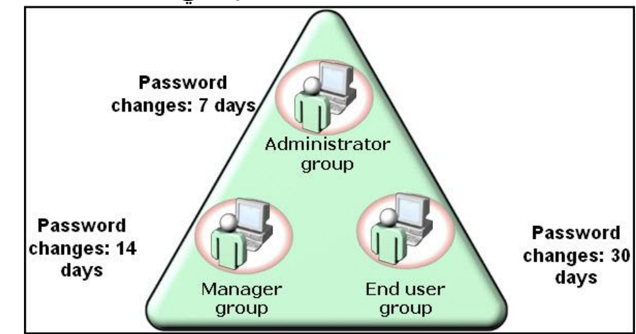
عدد مرات الدخول خطا للحساب
يفضل ان تكون من ٣ الي ٥ مرات ولا تزيد عن هذا



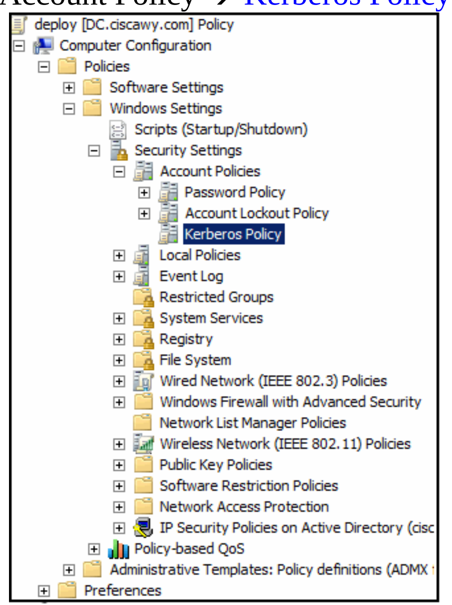
-: Reset account lockout counter after

الفتره التي يتم بعدها اعاده محاوله المستخدم للدخول الي حسابه
By-default 30 دقيقه

- يفضل في ميكروسوفت تطبيق بعض الPolicies المعقده اكثر علي حسابات المستخدمين



Computer Configuration → Policies → Windows Setting → Security Setting
Account Policy → Kerberos Policy



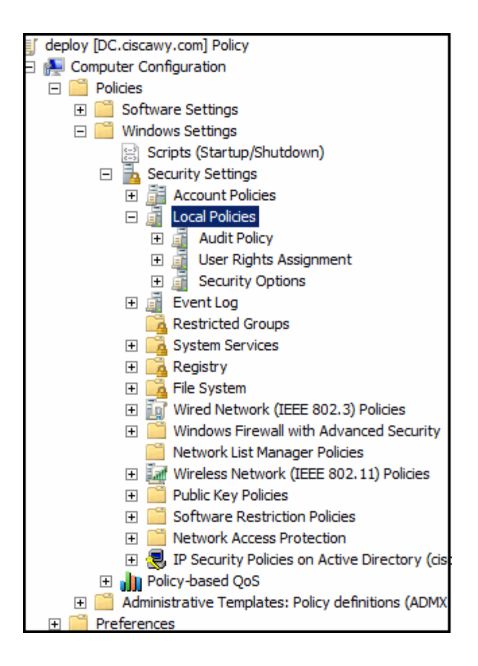
تهتم بالبروتوكول الخاص بعمليه تشفير كلمات المرور و هو الkerberos Protocol

Kerberos Authentication in an Active Directory Domain

In an Active Directory domain, the Kerberos protocol is used to authenticate identities. When a user or computer logs on to the domain, Kerberos authenticates its credentials and issues a package of information called a *ticket granting ticket* (TGT). Before the user performs a task such as connecting to a server to request a document, a Kerberos request is sent to a domain controller along with the TGT that identifies the authenticated user. The domain controller issues the user another package of information called a *service ticket* that identifies the authenticated user to the server. The user presents the service ticket to the server, which accepts the service ticket as proof that the user has been authenticated.

These Kerberos transactions result in a single network logon. After the user or computer has initially logged on and has been granted a TGT, the user is authenticated within the entire domain and can be granted service tickets that identify the user to any service. All of this ticket activity is managed by the Kerberos clients and services built into Windows and remains transparent to the user.

Computer Configuration → Policies → Windows Setting → Security Setting
Account Policy → Local Policy



الخاصه ببعض الPolicies علي الLocal Account

Computer Configuration → Policies → Windows Setting → Security Setting
Account Policy → Local Policy → Audit Policy

- خاصه بعمليات المراقبه للمستخدمين ومعرفه مواعيد الدخول والخروج وما الأدوات التي تم استخدامها من قبل المستخدم
- اهميتها في اجراء عمليات المراقبه او الTShoot وأيضا اذا حدث Error علي الServer يتم من خلالها معرفه من من المستخدمين كان متواجد في وقت حدوث هذا الخطأ
- يستخدم الTool Event Viewer لأجراء عمليه ال Monitor

Start → Administrative tools → Event Viewer

Computer Configuration → Policies → Windows Setting → Security Setting
Account Policy → Local Policy → Uesr Rights Assignment

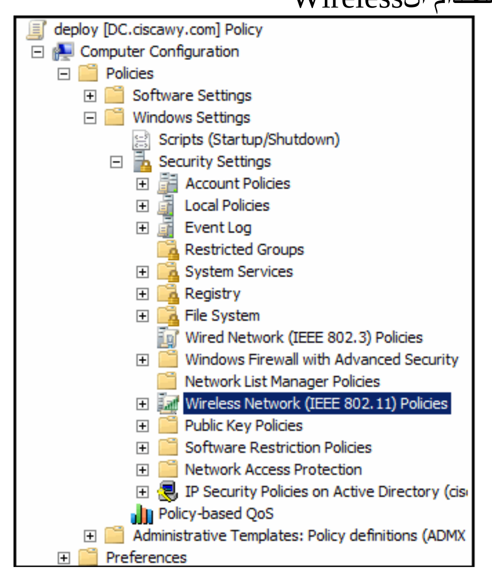
بها كل الPolicies والنقيض لها .. اي انه عند تطبيقها لن تجد إلا خيار واحد
وعلي حسب ما تريد تطبيقه تستخدم الPolicy
وبعض ال Policies الاخري التي يمكن أن تحتاجها فيما بعد

Computer Configuration → Policies → Windows Setting → Security Setting
Account Policy → Local Policy → Security Options

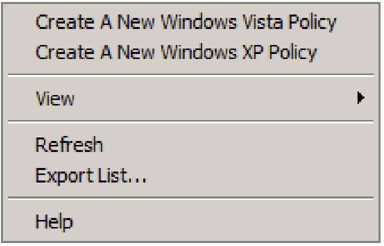
بعض الاختيارات الخاصه بالحساب الشخصي
يمكن ان :-
Accounts: Rename administrator account ⇦ إعاده تسميته
Interactive logon: Do not require CTRL+ALT+DEL ⇦ أي ألا يتم عمل Lock للAccount بعد فتره معينه (تعتبر احدي اساليب الحمايه) حتي لا يظل الحساب مفتوح يستخدمه أي احد
Interactive logon: Message text for users attempting to log on ⇦ يمكن ان اضيف رساله لكل المستخدمين، كتنويه عن شئ ما أو تهنئة بمناسبه عامه

User configuration → Admin Templete → System → Removable Storage Access
يمكن من خلالها اتحكم في مداخل الUSB أو CD and DVD removable storage او أي Removable Storage
هناك اختيارين يتم التعامل معهما
Denies read access ⇦ أي لا يتم قراءة محتوياتها
Denies write access ⇦ يتم قراءة المحتويات ولكن لا يسمح بالتعديل بها

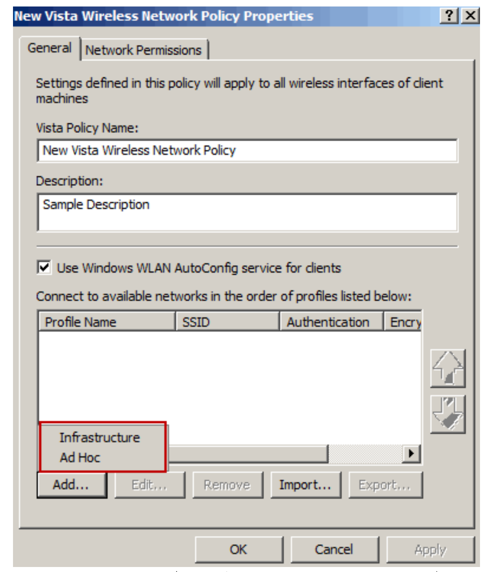
Computer Configuration → Policies → Windows Setting → Wireless Network Policy
للتحكم في الدخول علي الانترنت بإستخدام الWireless



تستخدم علي كل من Windows XP او Viste – 7

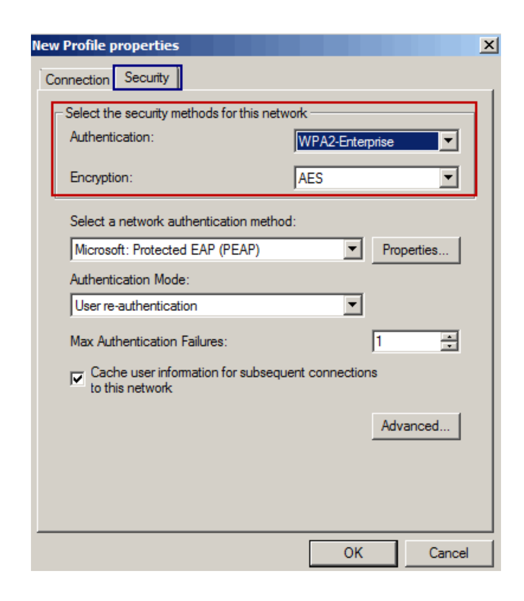


سنقوم بتطبيقها علي New Vista Wireless Network Policy
ستظهر لنا هذه الشاشه
نقوم بالضغط علي Add لإضافه نوع الConnection



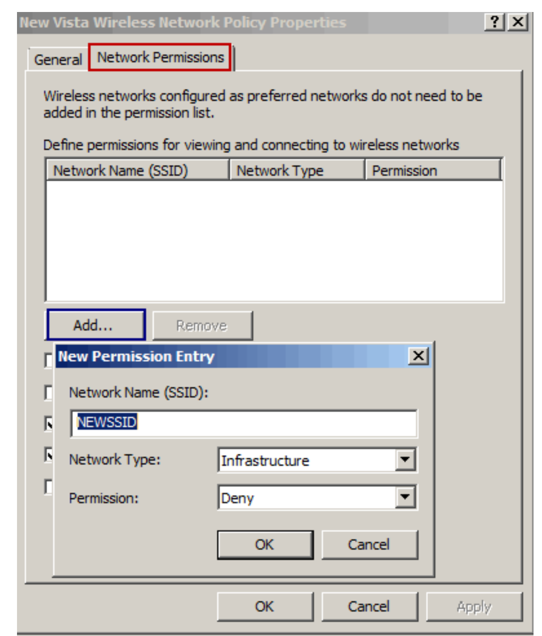
Add Hock :- تستخدم بين جهازين متصلين ببعضهما تشبه كثيرا الPeer – to – Peer
Infrastructure :- نفس فكره عمل الSwitch مجموعه اجهزه متصله ببعضها
نختار احداهما ثم نضغط Ok

نختار Security Tab



هذه مخصصه بانواع الAuthentication وانواع التشفير
افضلهما في الوثوقيه الWPA2-Enterprise يصعب كسره واختراقه
والتشفير TKIP
وهذه الخيارات تترك لك انت كمدير للنظام علي حسب السياسه التي تتبعها الشركه
كما قلت من قبل ليس هناك خطوات محدده في الPolicy انما هي Going Throw بعضعهما لتوسيع الافق لك

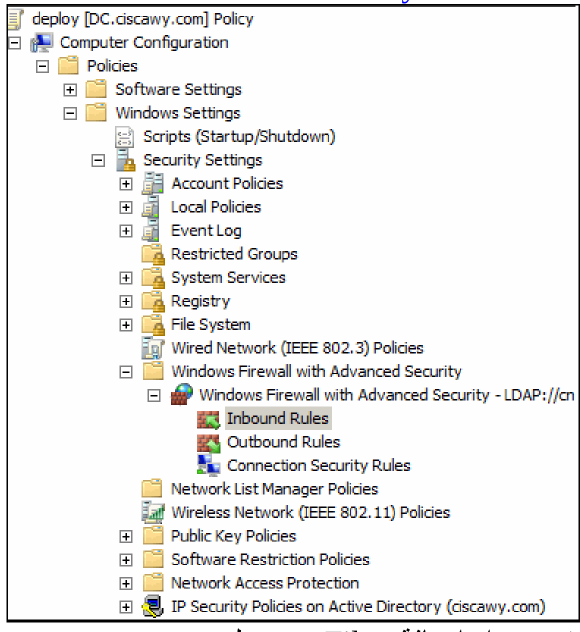
نختار Network Permission من فوق



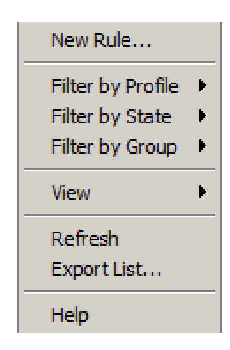
ونضغط علي Add ونضيف الSSID
الSSID الأسم الخاص بالAccess Point التي من خلاله يستطيع المستخدمين استخدام الانترنت
يمكن ان نضيف اكثر من Access Point ونجري بينهما Load Balance لتجنب حدوث ضغط علي الانترنت وبالتالي يحدث Load علي الشبكه ونفقد الاتصال
ونتحكم في مواعيد استخدام الUser لأين منهما

- Windows Firewall

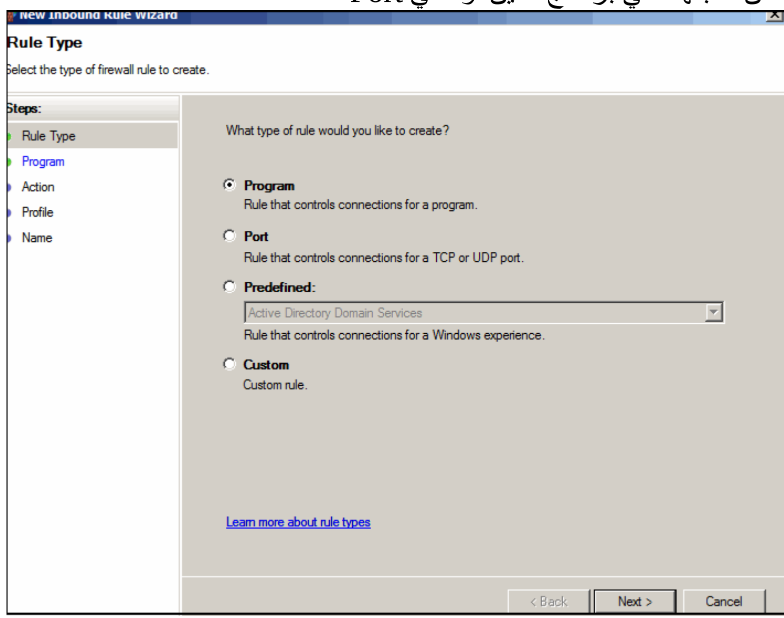
Computer Configuration → Policies → Windows Setting → Windows Firewall and Advanced Security



يمكن اضافة أي Role علي المستخدمين او اضافة Filter معين عليهم
R.click → New Role

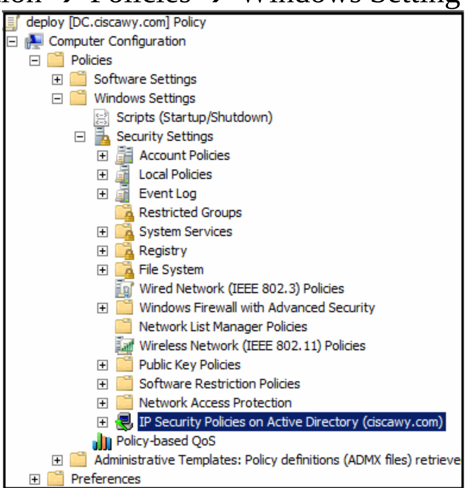


ونختار اي Role نريد ان تطبقها علي برنامج معين او علي Port محدد

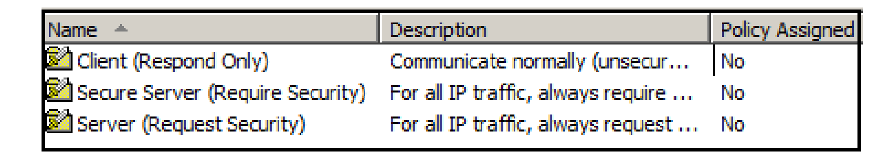


- IP Security

Computer Configuration → Policies → Windows Setting → IP Security Policy



ثلاثة أنواع :-

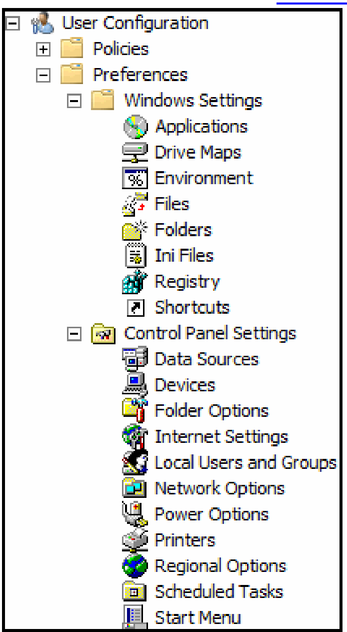


Name	Description	Policy Assigned
Client (Respond Only)	Communicate normally (unsecur...	No
Secure Server (Require Security)	For all IP traffic, always require ...	No
Server (Request Security)	For all IP traffic, always request ...	No

Response	**ممكن ان يكون الاتصال Secure او نستخدم اتصال عادي**
Require Security	لابد ان يكون الاتصال Secure
Request Security	هيحصل عملية تفاوض في اول الاتصال ان يكون Secure واذا لم يتم الاستجابه يستخدم اتصال عادي ولكن كل فتره سيتم التنويه علي ان يستخدم Secure Connection

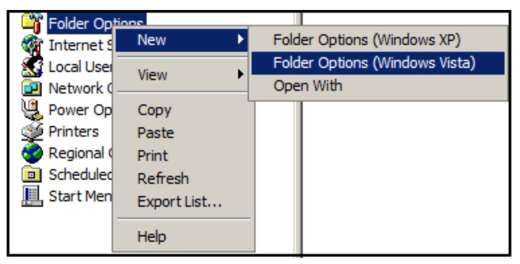
▪

User Configuration → Preferances → Windows Setting
User Configuration → Preferances →Control Panal Setting

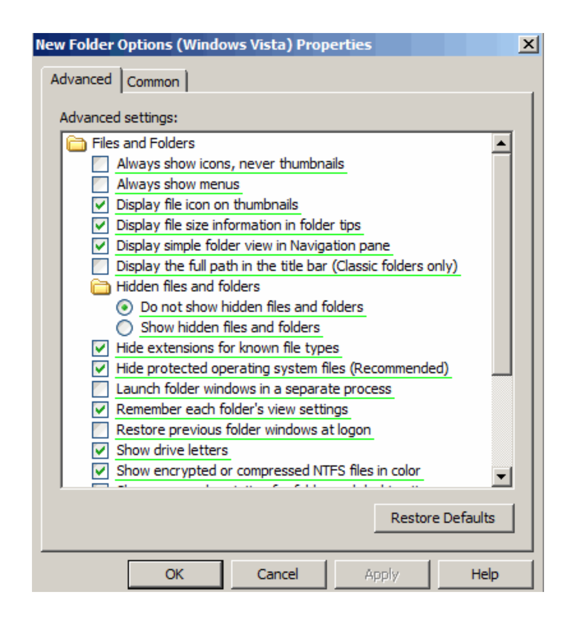


يمكن من خلالهما ان اتحكم في مكونات الوندوز والتحكم في سطح المكتب ويمكن ان اضيف تعريف لأي Device او غلق برنامج او حساب للمستخدم او تعريف Printer علي كل الاجهزة

نختار مثلا الFolder Options



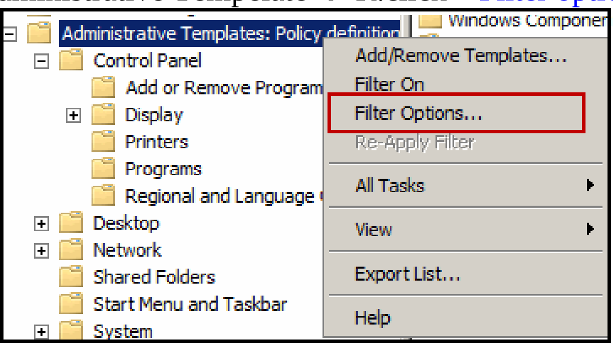
ونختار Folder Options Windows Vista



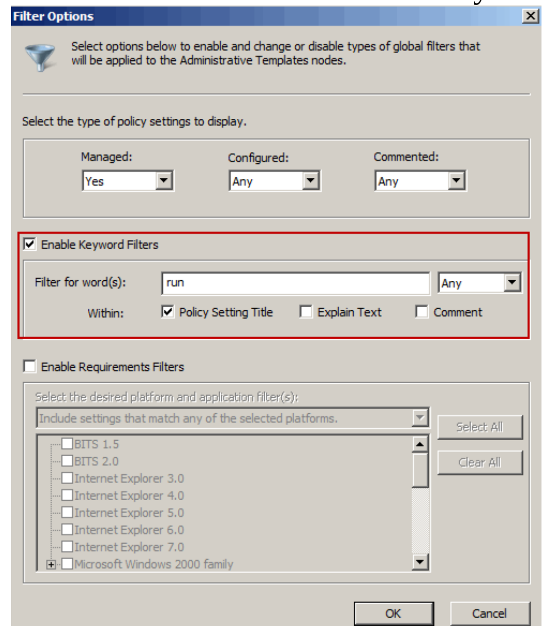
وتختار اي Option تريده

▪

يمكن ان اضيف Filter ليسهل عمليه البحث عن الPolicy التي اريد تطبيقها بكتابة أي كلمه دلاليه
Administrative Tempelate → R.click – Filter option

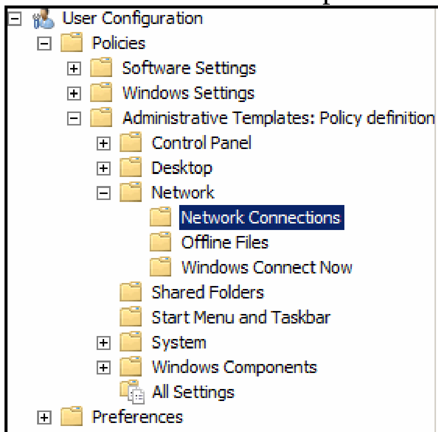


نكتب الكلمه الدلاليه التي نريد البحث عنها
ولكن يفضل الا يتم وضع ✓ علي كل من Explain text و الComments لإنه سيتم البحث عن كل شئ
وتترك ال✓ علي الPolicy Setting Tittle فقط



Lab

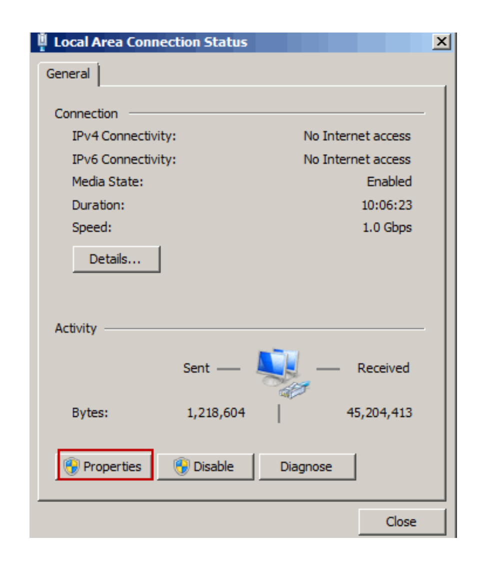
User configuration → Policies→ Admin template → Network Connection



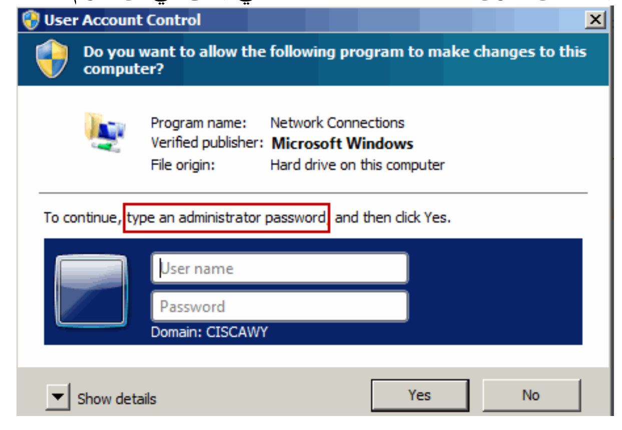
Prohibit TCP/IP advanced configuration Enabled No

أمنع المستخدم من انه يعدل في إعدادات الTCP/IP
ثم اقوم بكتابه gpupdate /force في RUN

- يتم الدخول بحساب المستخدم المطبق عليه هذه الPolicy
ندخل علي هذا المسار
Control Panel\Network and Internet\Network and Sharing Center
ونضغط علي Properties



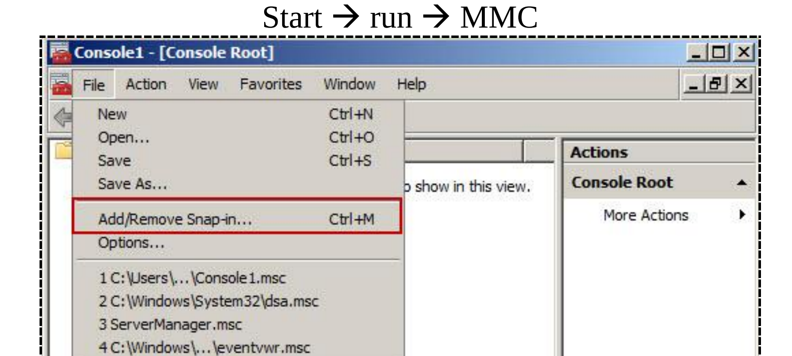
ستظهر لنا هذه الصوره تفيد انه يجب ان اكون Administrator حتي يحق لي ان اقوم بهذا التعديل



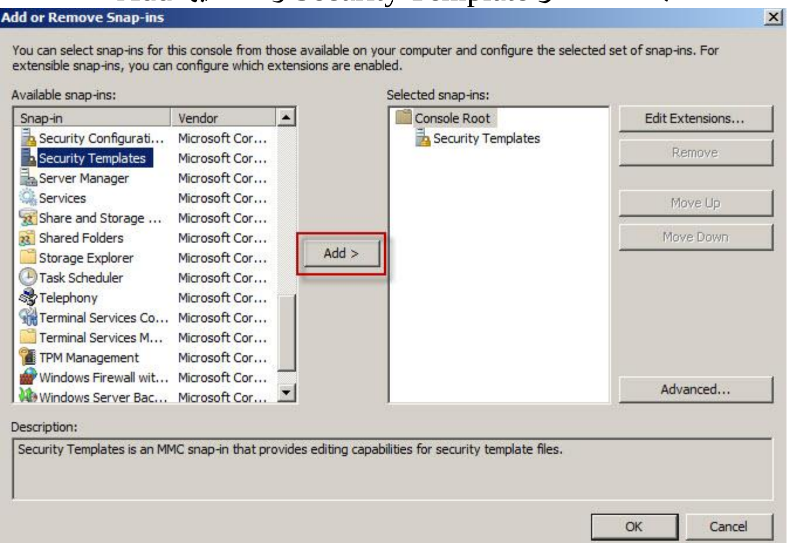
Group Policy Template

- يمكنني ان اقوم بعمل Template لبعض الPolicies التي اريد تطبيقها ،، او أحملها من علي الانترنت وعمل Import لها من داخل الGroup Policy
- وذلك لتسهيل وسرعة تطبيق الPolicies المحدده وعدم الخوض في كل عناصر الGroup Policy حيث ان الTemplate بها بعض الPolicies المحدده التي نستخدمها باستمرار

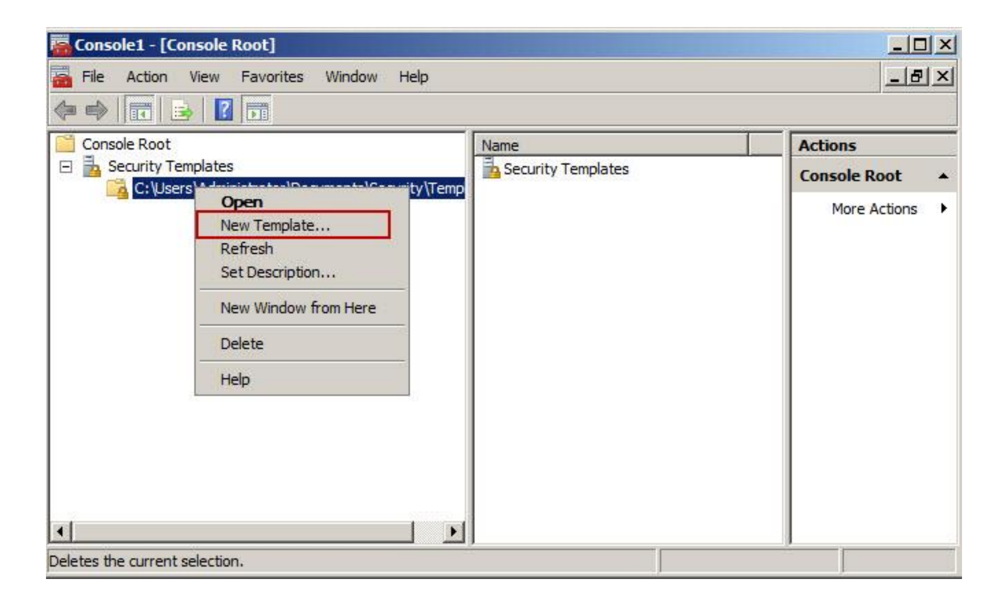
Start → run → MMC



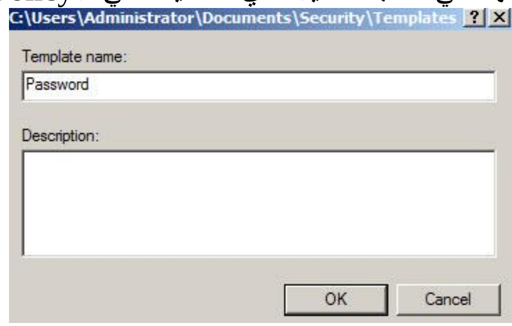
بعد كدا نختار Security Template ونعمل ليها Add



نقوم بفتحها ثم R.click → New Template

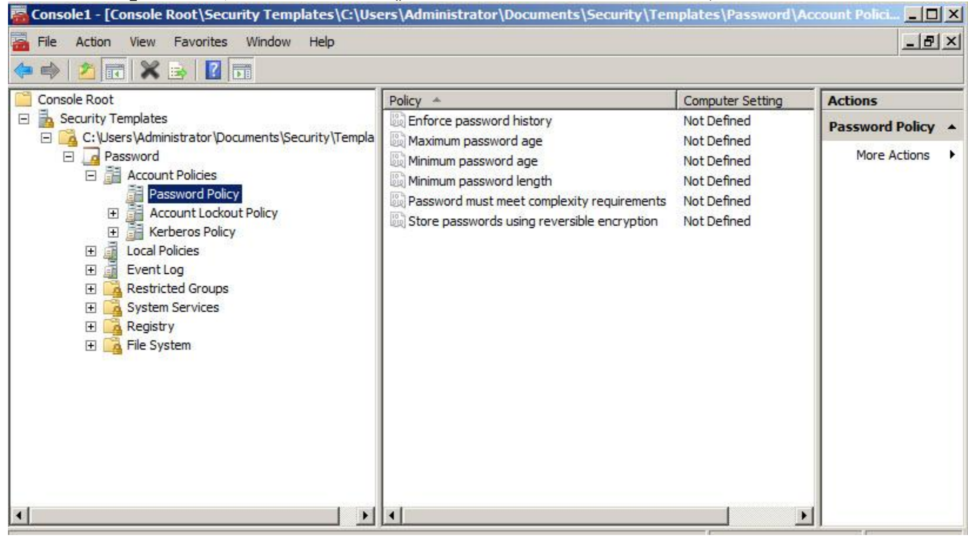


نختار اسم لها علي حسب التعديل الذي سنضيفه علي الGroup Policy

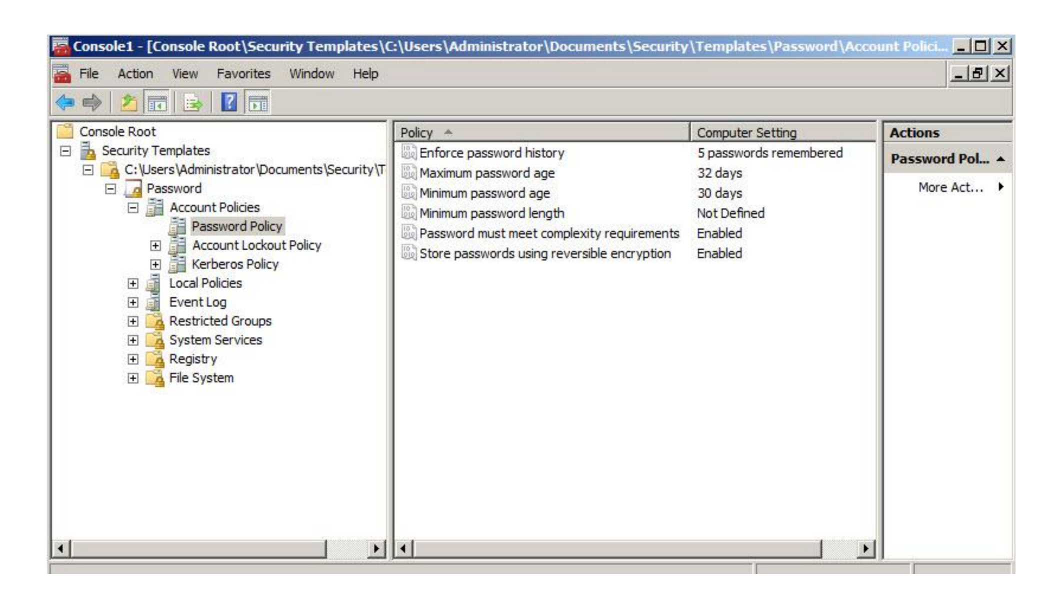


دي الPolicy قبل ما اعدل فيها اي حاجه

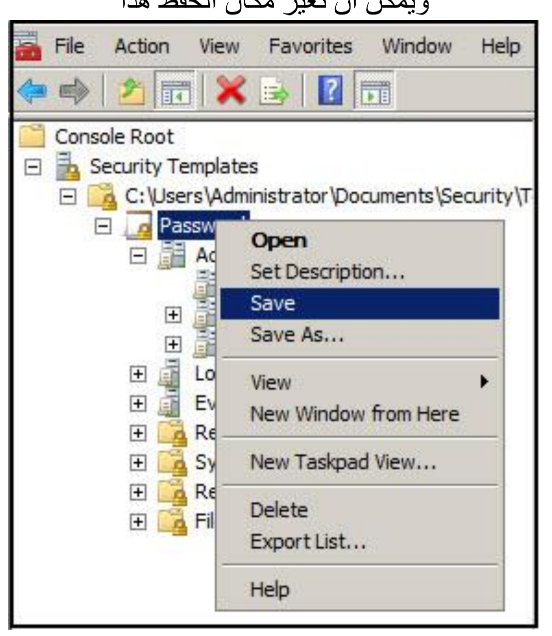
ويمكنك ان تختار اي عنصر آخر من المدرجين علي اليسار تحت اسم الTempelete



عدلت في ال Policy بعض الخصائص



وجاءت الآن مرحله الSaving
تلقائيا تحفظ الTemplate في ملف يسمي Templates
C:\Users\Administrator\Documents\Security\Templates
ويمكن ان نغير مكان الحفظ هذا



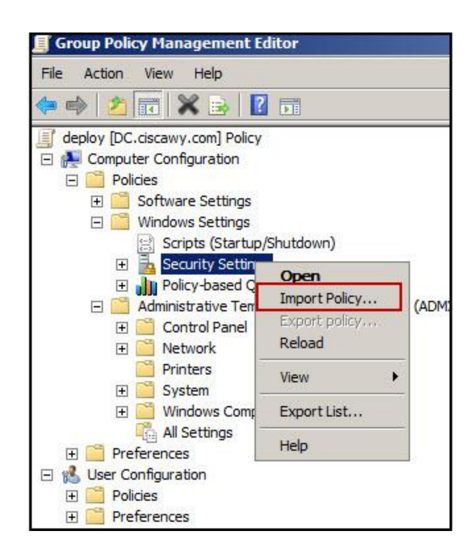
Security templates

Allow you to configure any of the following types of policies and settings:

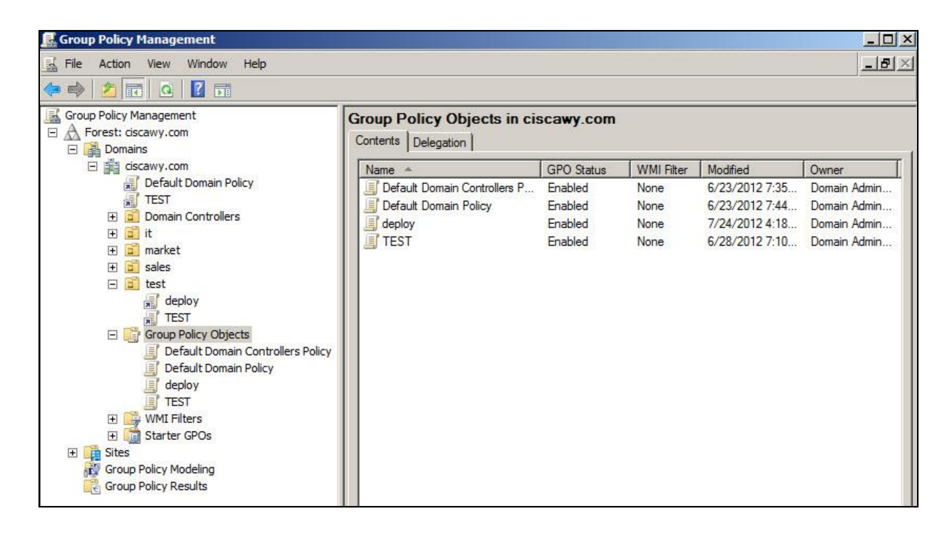
- Account Policies Specify password restrictions, account lockout policies, and Kerberos policies.
- Local Policies Configure audit policies, user rights assignments, and security Options policies.
- Event Log Policies Configure maximum event log sizes and rollover policies.
- Restricted groups specify the users permitted to be members of specific groups.
- System Services specify the startup types and permissions for system services.
- Registry Permissions Set access control permissions for specific registry keys.
- file System Permissions Specify access control permissions for NTFS files and folders

لتفعيل الTempleteـ :-

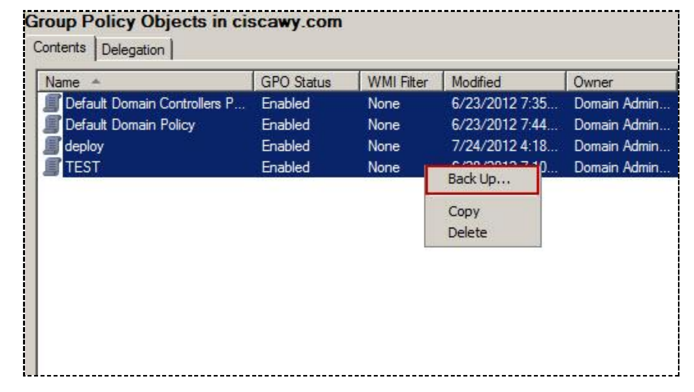
- نقوم بفتح الGroup Policy Management
- ثم نقوم بفتح الPolicy المراد التعديل فيها واضافه الTemlete الجديده
- نقوم بفتح الSecurity Setting ونضغط R.click → Import Policy
- ستخدن انه تم وضعها تحت العنوان الخاص بها
- ثم تقوم بعمل gpupdate



Group Policy Object



من خلالها يمكنني ان اقوم بعمل Back up لكل الPolicies المطبقة علي الDomain او لأحداهما فقط

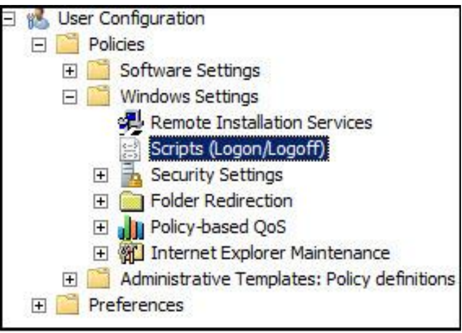


- لتطبيق script معين علي كل المستخدمين أو عمل Shared Folder لمستخدم معين حينما يستخدم أي Computer Account يري كل الشغل الخاص به
- تطبق الscript علي كل من الUser and Computer Account

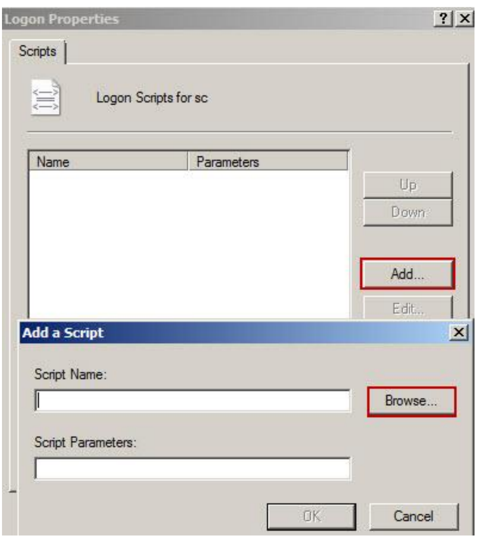
USER ACCOUNT	COMPUTER ACCOUNT
• Log on • Log off	• Start up • Shut down

- نقوم بعمل Shared Folder علي السيرفر وليكن مثلا X او اي اسم
- نقوم بفتح الGroup Policy Management
- نقوم بعمل Edit علي الPolicy التي ستطبق علي المستخدم

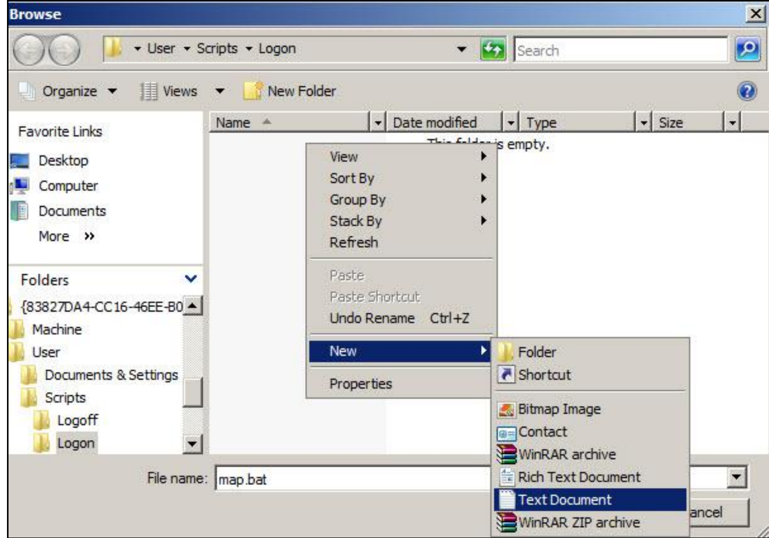
User configuration → Policies → windows setting → scripts



R.click on logon → Properties
ونضغط علي Add ومنها Browse

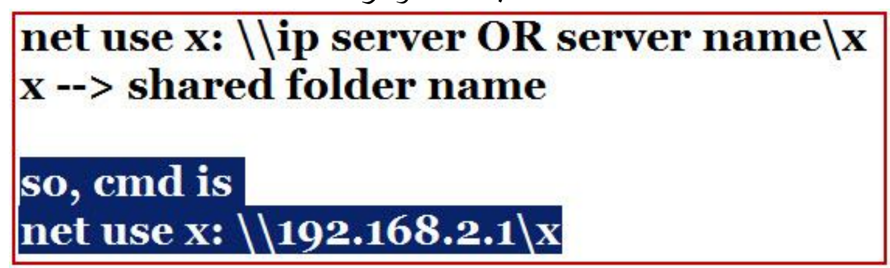


R.click → New text



نسميه اي اسم نريده ولكن يشترط ان يكون .bat أي batch file

R.click علي الملف ونختار Edit ونضغط علي Run
لكتابه هذه الاوامر

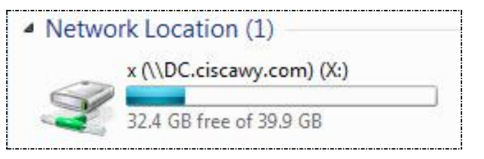

net use x: \\ip server OR server name\x
x --> shared folder name

so, cmd is
net use x: \\192.168.2.1\x

هناك امر آخر اختياريا و هو
Net use administrator p@ssw0rd
حتي يكون الadministrator فقط هو من له صلاحيه الولوج الي هذا الملف
ثم نضغط علي open ومنها ok

- نقوم الان بالدخول علي جهاز ال٧ وندخل بحساب المستخدم الطبق عليه هذه الPolicy ونفتح My Computer

سنجد ان هناك Map Drive تمت اضافته



Backup & Restore

- ❖ يجب ان نجري بإستمرار عمليه Backup لكل محتويات الDomain الخاص بنا لتجنب حدوث أي فقد في الداتا او في الInfra الخاصه بالDomain
- ❖ و هي عباره عن نسخه احتياطيه عليها كل البيانات يتم تخزينها وحفظها حتي اذا حدث فقد في اي شئ يسهل استرجاعه ولا يحدث ضرر او فقد لأي Critical volumes
- ❖ يجب ان يكون هناك Drive خاص للBackup

Critical volumes include:

- The system volume: the volume that hosts the boot files
- The boot volume: the volume that hosts the Windows operating system and the Registry
- The volume that hosts the SYSVOL tree
- The volume that hosts the AD DS database (Ntds.dit)
- The volume that hosts the AD DS database log files

- أنواع الBackup :-

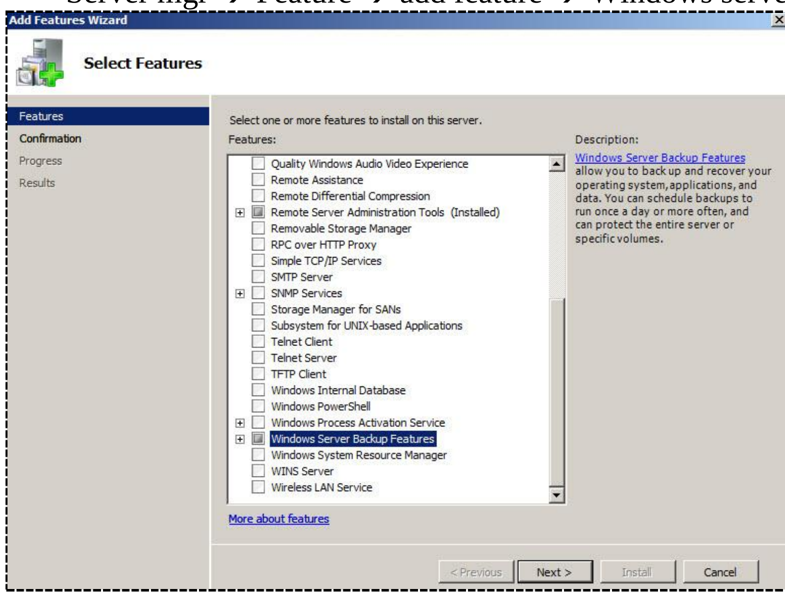
Backup جزئي و هو يأخذ كل اسبوع او كل شهر
Backup كلي و هو يأخذ كل عام
حتي نتجنب حدوث اي فقد في أي Object خاص بالDomain

- يفضل ان يحفظ الBackup في اماكن مختلفه :-

- في نفس المؤسسه الموجود بها الDomain .
- في احدي البنوك التابعة للمؤسسه .
- في بلد اخري غير الموجود بها .
حتي اذا حدثت اي كارثه طبيعيه كما حدث في اليابان إعصار تسونامي يكون لدنيا نسخه احتياطيه من كل الداتا

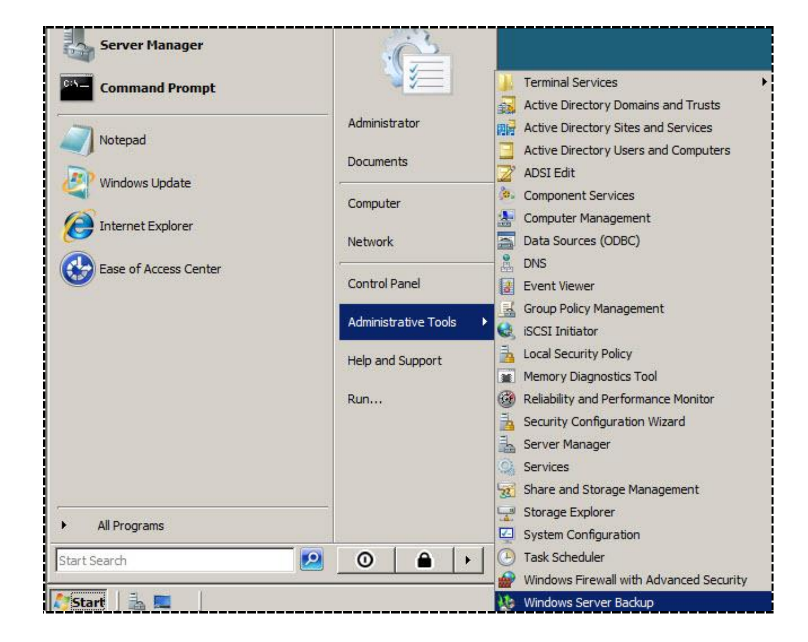
- يتم اضافه Drive جديد علي السرفر الذي نريد ان نأخذ منه Backup
- لتفعيل خاصية الBackup :-

Server mgr → Feature → add feature → Windows server backup Feature

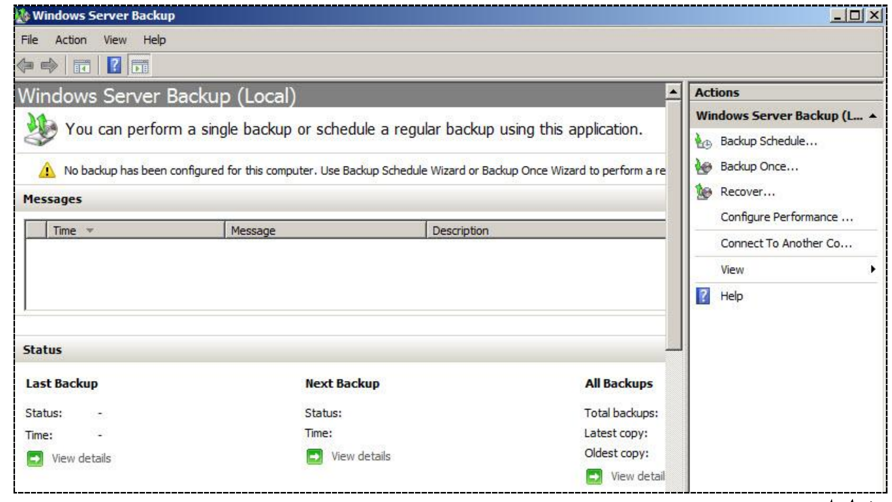


Next → Install → Finish

سأقوم الآن بأخذ نسخه احتياطيه من الDomain
Start → administrative tools → windows server backup



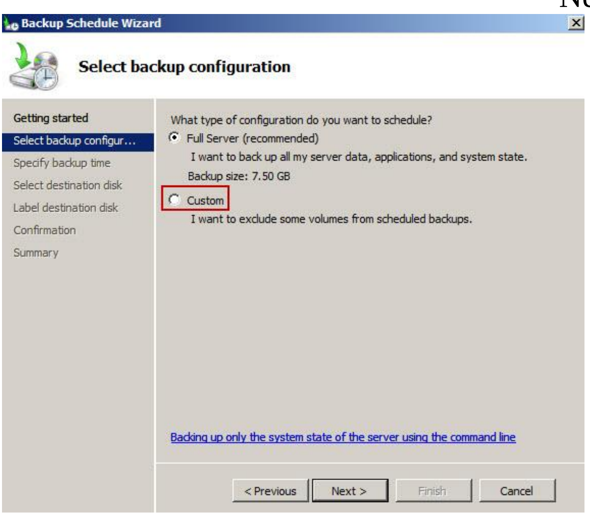
ستظهر لنا هذه الشاشه



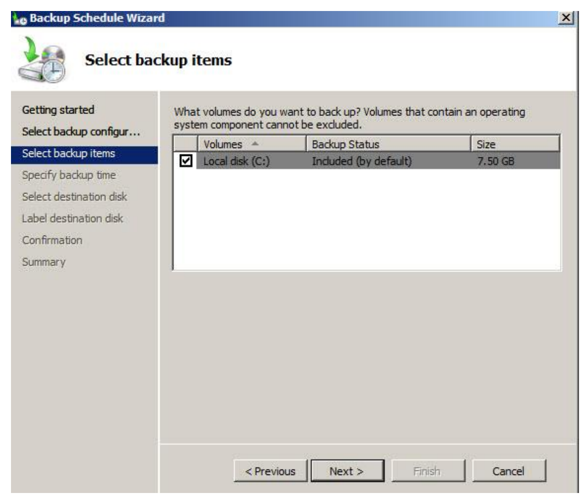
سنجد عندك عده اختيارات

Backup Schedule -: وهو انك تحدد اوقات معينه لإجراء عمليه الBackup وتعتبر من أساسيات الBackup الجزئي حيث يتم الإعتماد عليها

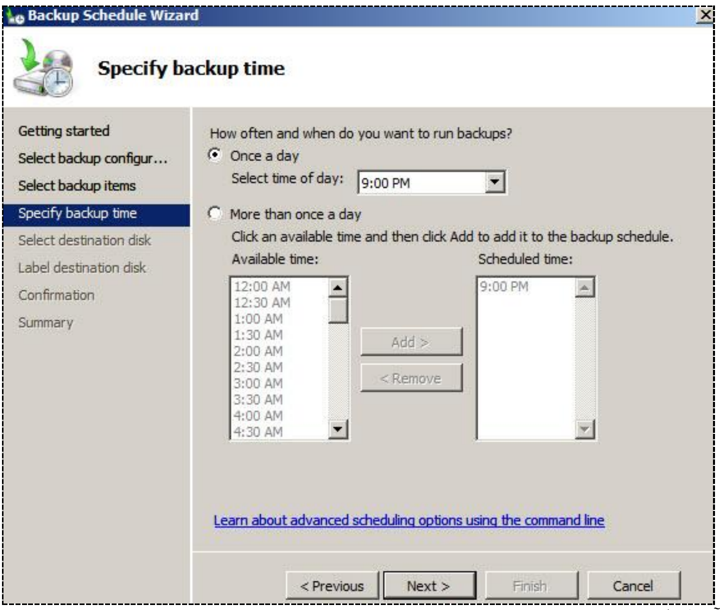
نقوم بالضغط عليها ثم نختار Next



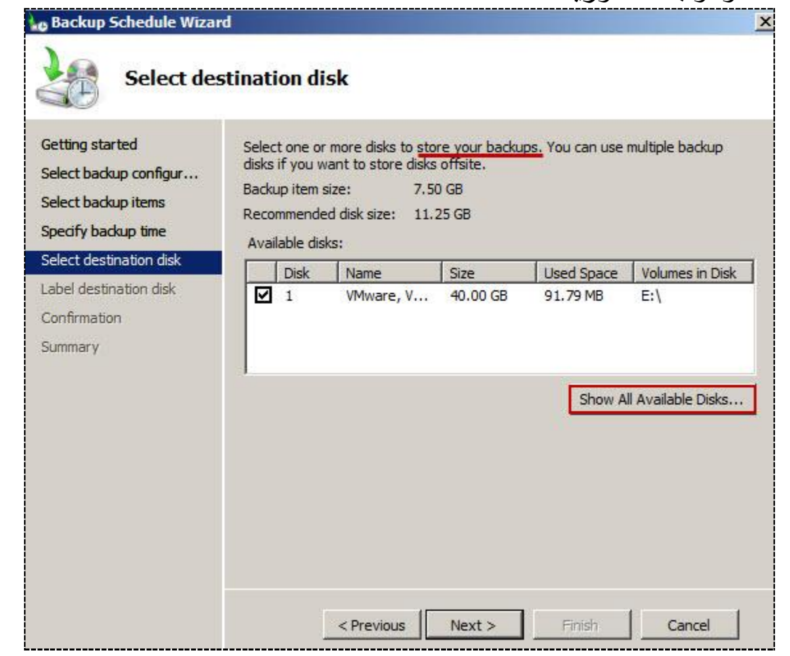
نختار Custom لإظهار خيارات متعدده اكثر



نختار الDrive المراد أخذ منه نسخه احتياطيه



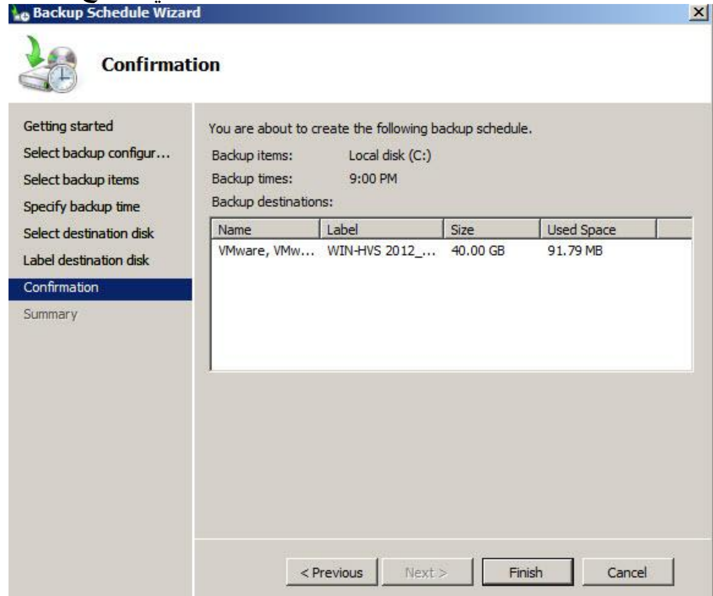
هنا نختار الأوقات المراد آخذ ال Backup فيها
سواء كانت مره واحده فقط او بصفه دوريه



نضغط علي Show All Availabe Disks عشان نختار منها الDisk اللي هيكون مكان تخزين الBackup



نفيد هذه الرساله انه بعد الانتهاء من هذه الاعدادات ان الDisk ســFormated حتي يصبح جاهزا لعمليه الBackup



Next ثم Finish

لكي نبدأ عمليه الBackup :-

نقوم بفتح cmd → Run

ونكتب ? wbadmin يتظهر لنا كل خصائص هذا الأمر

نختار منها START BACKUP

واذا أردنا ايقاف العمليه نضغط علي ctrl+c

```
C:\Users\Administrator>wbadmin
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.


ERROR - Command incomplete. See list below.
For more help, type wbadmin <command> -help

---- Commands Supported ----

ENABLE BACKUP              -- Enable or modify a scheduled daily backup
DISABLE BACKUP             -- Disables running scheduled daily backups
START BACKUP               -- Runs a backup
STOP JOB                   -- Stops the currently running backup or recovery
GET VERSIONS               -- List details of backups recoverable from a
                              specific location
GET ITEMS                  -- Lists items contained in the backup
START RECOVERY             -- Run a recovery
GET STATUS                 -- Reports the status of the currently running job
GET DISKS                  -- Lists the disks that are currently online
START SYSTEMSTATERECOVERY  -- Run a system state recovery
START SYSTEMSTATEBACKUP    -- Run a system state backup
DELETE SYSTEMSTATEBACKUP   -- Delete system state backup(s)

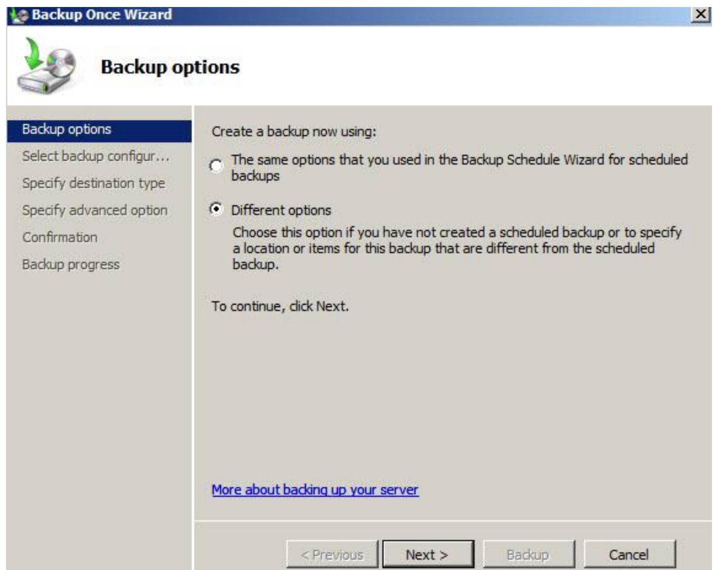
C:\Users\Administrator>wbadmin START BACKUP
wbadmin 1.0 - Backup command-line tool
(C) Copyright 2004 Microsoft Corp.

Do you want to run a backup using the same configuration you use for scheduled
backups?
[Y] Yes [N] No y

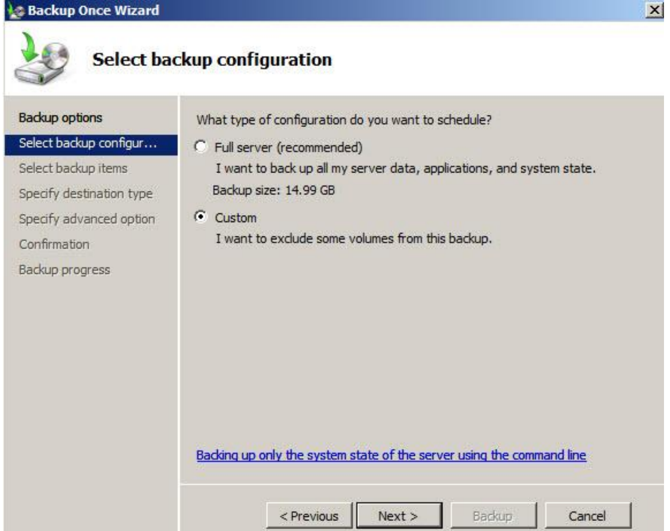
Backup to Scheduled backup target is starting.
```

نذهب مرة اخري الي Windows Server Backup :-

نختار Backup Once



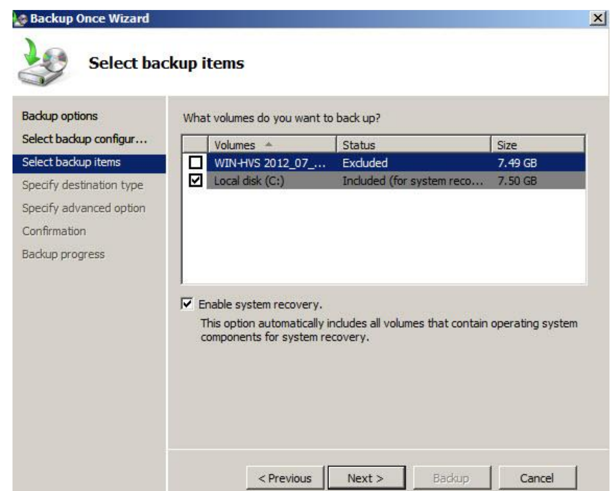
نختار الاختيار الثاني ،، لأننا لو قمنا بالإختيار الاول سيقوم بإجراء عمليه Backup طبقا للإعدادات التي تم أخذها في الSchedule

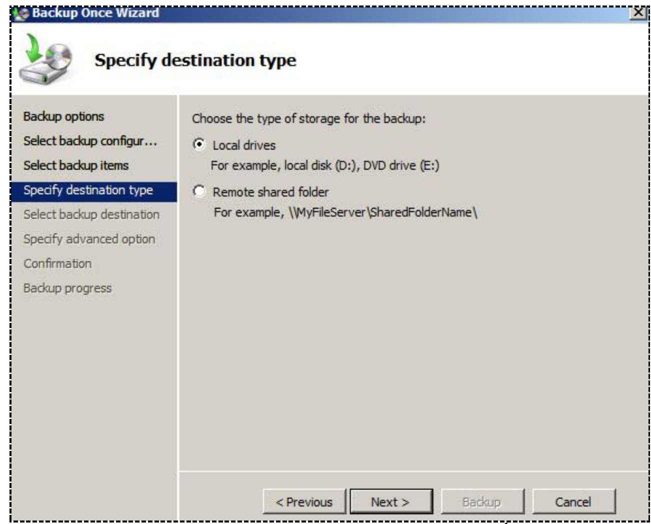


هنختار Custom

والاختيار الاول معناه أننا سنأخذ نسخه من كل الملفات الموجوده في ال:\C

اما Custom سيتيح لنا اختيار ملفات محدده





مكان حفظ النسخه ستكون علي نفس الجهاز أم علي Shared Folder

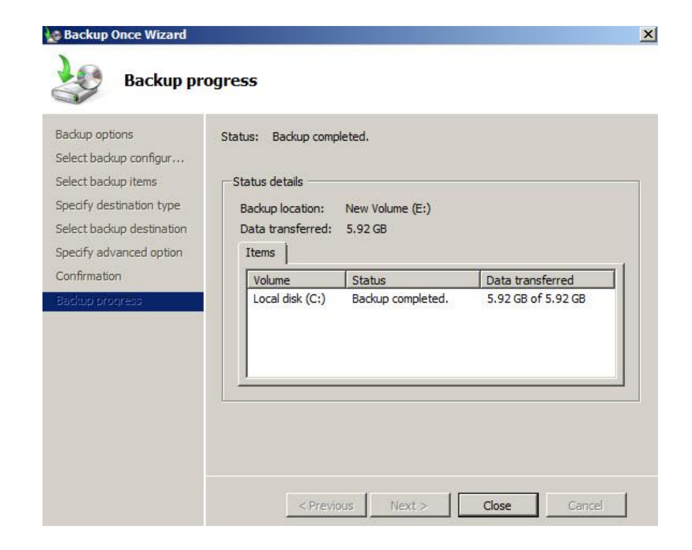
اختار Local

يتم اختيار الخيار الثاني في حالة اخذ نسخه احتياطيه من اجهزة الClients الموجودين واريد ان يتم حفظهم كلهم في مكان واحد



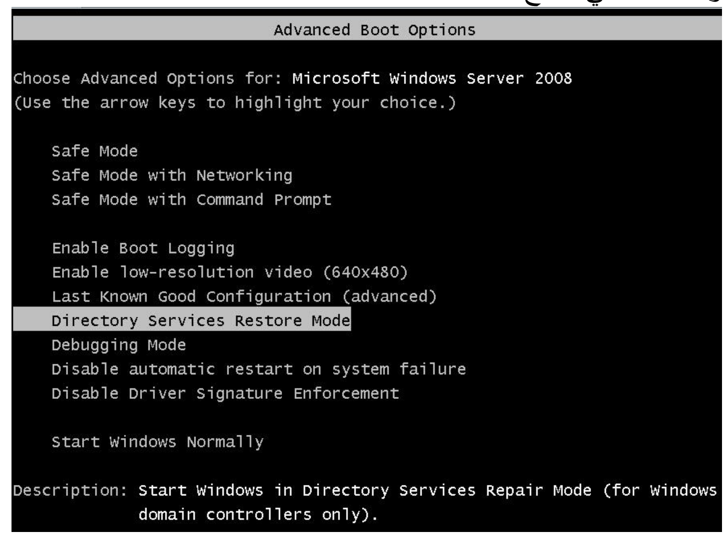
نقوم بإختيار الDisk

ثم نقم بالضغط علي Next ثم Backup



بعد الانتهاء من عمليه الBackup تأتي الان خطوات ال Restore :-

نقوم بإعاده تشغيل الجهاز والضغط علي مفتاح F8



Restarting in DSRM

There are two ways to launch a server into DSRM. The first relies on a server reboot and, during the reboot process, pressing F8 to view startup options. Note that if you are running the DC in a virtual machine on Hyper-V, you must press the F5 key while the machine is starting to access the Windows Boot Manager screen first, then press F8 to access Advanced Boot Options. This allows you to choose the Directory Services Restore Mode. Remember that you need to have access to the DSRM password to use this mode.

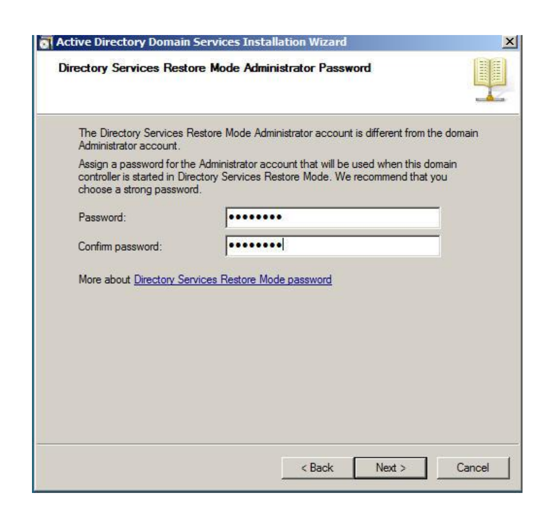
نختار Directory Services Restore Mode الخاصه بعمليه الRecovery



سيطلب مني صلاحيات الدخول

سنقوم بإعطاءه كلمه المرور التي قمنا من قبل بادخالها اثناء عمليه ترقيه dcpromo
التي كانت في هذه الخطوه تحديدا

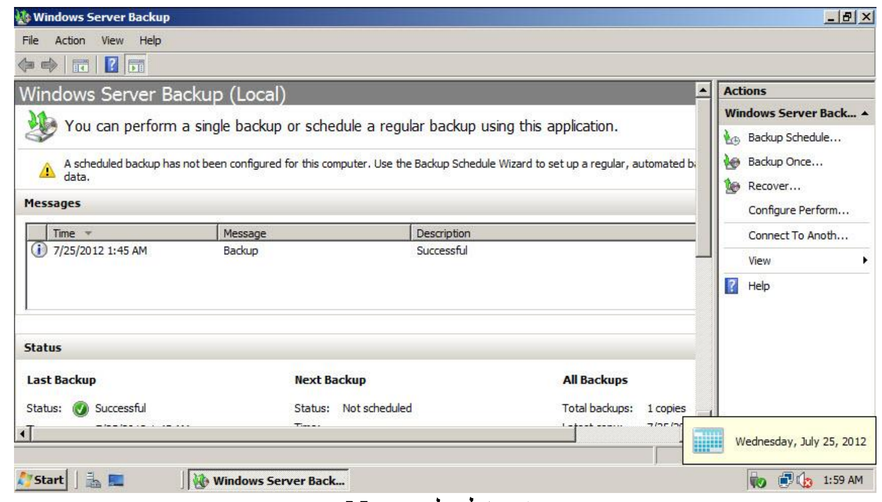
ولكن لماذا نقوم بالدخول بهذه الصلاحيات !!
نحن الآن نقوم بعمليه Restore للDomain ككل وكلمات المرور الخاصه بالمستخدمين و الخاصه بالAdministrators
مخزنه علي الDatabase الخاصه بالDomain
وحيث ان الDomain به عطل الآن ،، فكيف ستتم عمليه الAuthentication



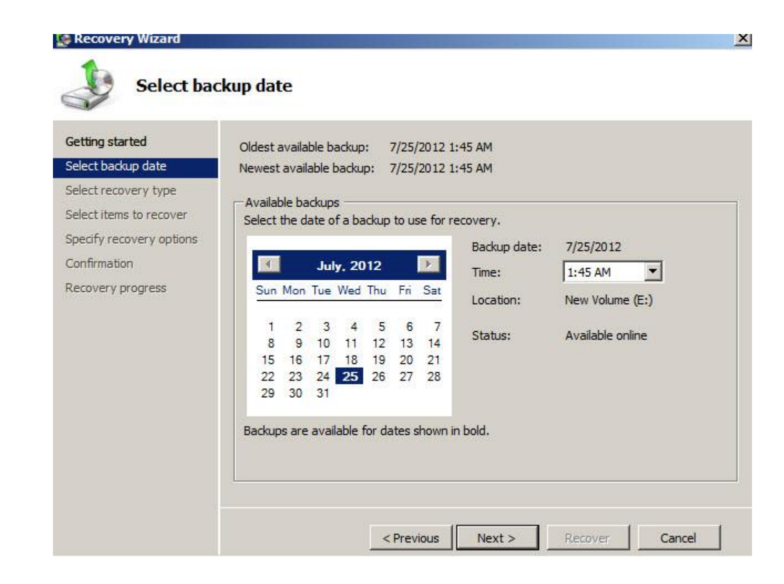
سنقوم بالدخول
سنجد ان كل الخدمات معطله ولن تستطيع عمل اي شئ



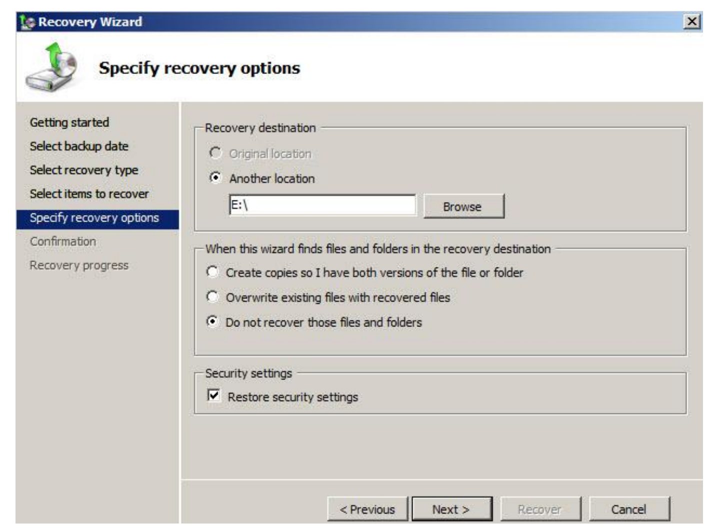
نقوم بفتح الWindows Server Backup
ونضغط علي Recover



ونضغط علي Next



نختار الوقت الذي تم اخد النسخه الاحتياطيه به
بعد ذلك نختار الملفات المراد عمل لها Recover
كل الملفات ام ملفات الDatabase فقط ام ملفات الSystem



نختار هنا مكان الRecovery Disk
وبعد ذلك Next ثم Recover
بعد اعادة التشغيل ستجد ان كل شئ عاد الي طبيعته

ملاحظه هامة
أحيانا قد يكون الBackup المقدم من ميكروسوفت غير مجدي ويحدث به بعض الاخطاء
لذا تجنب ان تعتمد عليه اعتمادا كليا واستخدم بعض الحلول الأخري ☺

الكتاب الثاني في كورس ال Active Directory

Course 6426A
Configuring and Troubleshooting Identity and Access Solutions with Windows Server 2008 Active Directory

وهو يتكلم عن 4 خدمات اساسيه هامه جدا :-

- **Active Directory Certification Authority**
- **Active Directory Federation Service**
- **Active Directory Light Weight Directory Service**
- **Active Directory Rights Management Service**

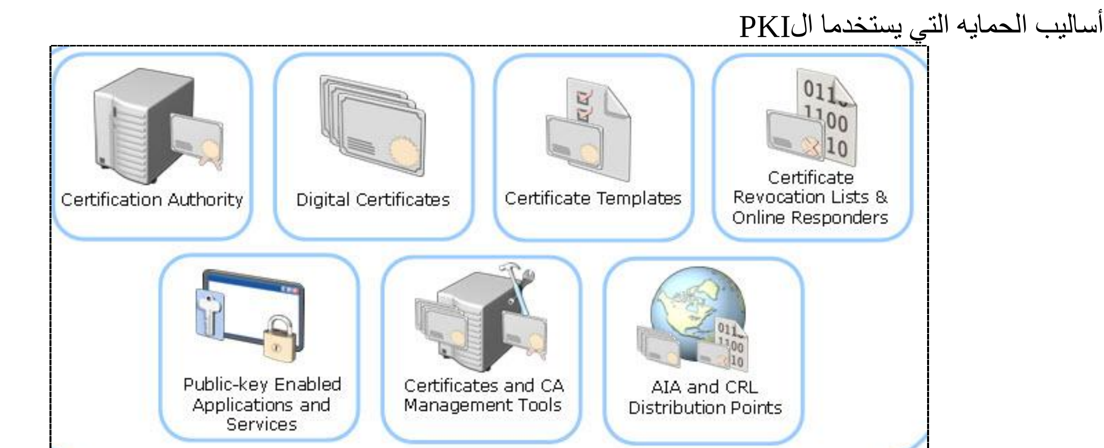
Active Directory Certification Authority

الغرض من استخدام هذه الخاصيه هي ضمان ان اي E-mails مرسله او اي Web Site يتم المستخدمين الموجودين في الشركه انهم موثوقين ولا يوجد فيهم اي مشاكل تضر بي

PKI → Public Key Infrastructure
مجموعه من الاساليب او المعايير او الآليات التي تستخدم Certification Authority او Digital Certification
الهدف منه ان يقوم بعمل تحكم وموثوقيه Authentication و Control علي جميع الاطراف المشاركه في ارسال البيانات

- Is the combination of software, encryption technologies, processes, and services that enable an organization to secure communication and business transactions
- Relies on the exchange of digital certificates between authenticated users and trusted resources

أساليب الحمايه التي يستخدما الPKI



يستخدم في
- Encryption
- IP Sec
- Securing Web Site
- Smart Card
- Signing Drivers

أنواع التشفير :-
- Symmetric اي تماثل
ان يكون التشفير Encryption وفك التشفير بإستخدام نفس ال Key
مثل AES, EDS, DES

- Asymmetric غير متماثل
يستخدم نوعين من الKeys
Public and Private إحداهما يستخدم في التشفير والآخر في فك عمليه التشفير
مثلRSA, DHA

HASH يقوم بعمل تشفير لل Password مستخدما MD5

Certification

Digital Certification يحدث لها عمليه Expire كل سنه (ويمكن التعديل فيها)
Certification Authority Server يحدث لها Expire كل ٥ سنوات (وأيضا يمكن التعديل فيها)
في الغالب يتم استخدام Asymmetric Key في عمليات التشفير

أنواع الCertification Servers

- Root CA

ينشأ لنفسه Self Sign Certificate
يكون هو الTrusted Server
يقوم بنشر وانشاء Physical Security & certification Issued Policy

- Subordinate CA

ينِشأ تحت الRoot CA
يستخدم في حاله عمل load balancing, and fault tolerance
او ان هناك تحميل علي الRoot

أنواع الCertification Authority

- Enterprise CAs

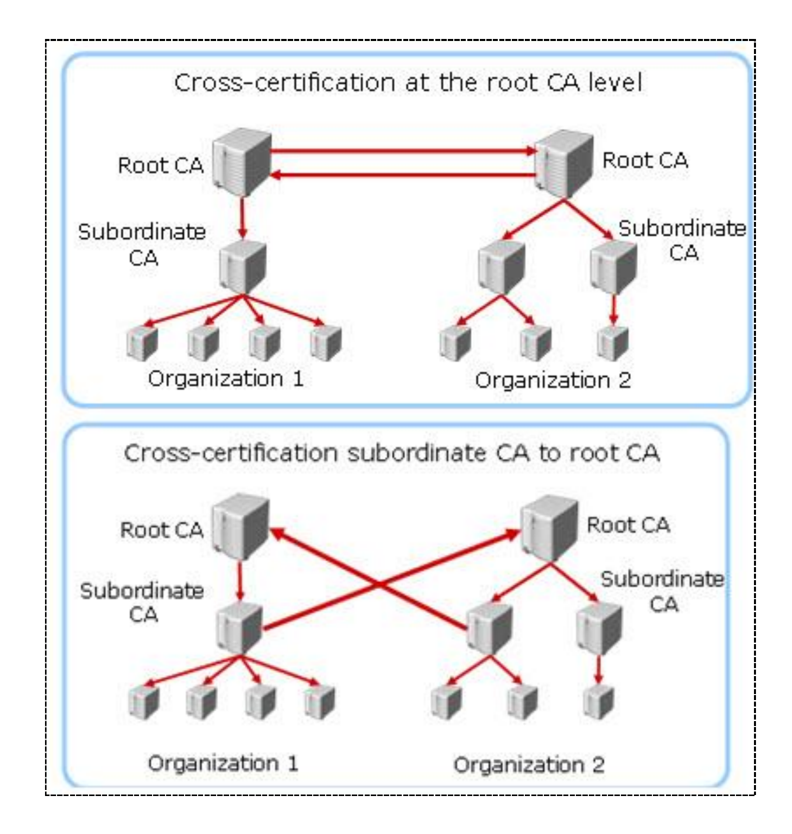
حينما نكون في بيئه عمل Domain

- Stand-Alone CAs

يمكن استخدامها في بيئه الWorkgroup

Stand-Alone CAs		Enterprise CAs	
	A stand-alone CA must be used if any CA (root or intermediate/ policy) is offline. This is because a stand-alone CA is not joined to an AD DS domain.		Requires the use of Active Directory®
			Requires AD DS
			Can use Group Policy to propagate certificate to Trusted Root CA certificate store
	Users provide identifying information and specify type of certificate		Publishes user certificates and CRLs to AD DS
	Does not require Certificate templates		Issues certificates based upon a certificate template
	All certificate requests kept pending till administrator approval		Supports autoenrollment for issuing certificates

Cross Hierarchy
أن اي مؤسسه يمكن ان تقوم بإنشاء اتصال مشفر مع الاخري



- Installing Certification Services

Server Mgr → Roles → Add Role

Server Manager

File Action View Help

Server Manager (CA)
Roles
Features
Diagnostics
Configuration
Storage

Roles

View the health of the roles installed on your server and add or remove roles and features.

Roles Summary — Roles Summary Help

Roles: 2 of 16 installed — Add Roles, Remove Roles

Active Directory Domain Services
DNS Server

Active Directory Domain Services — AD DS Help

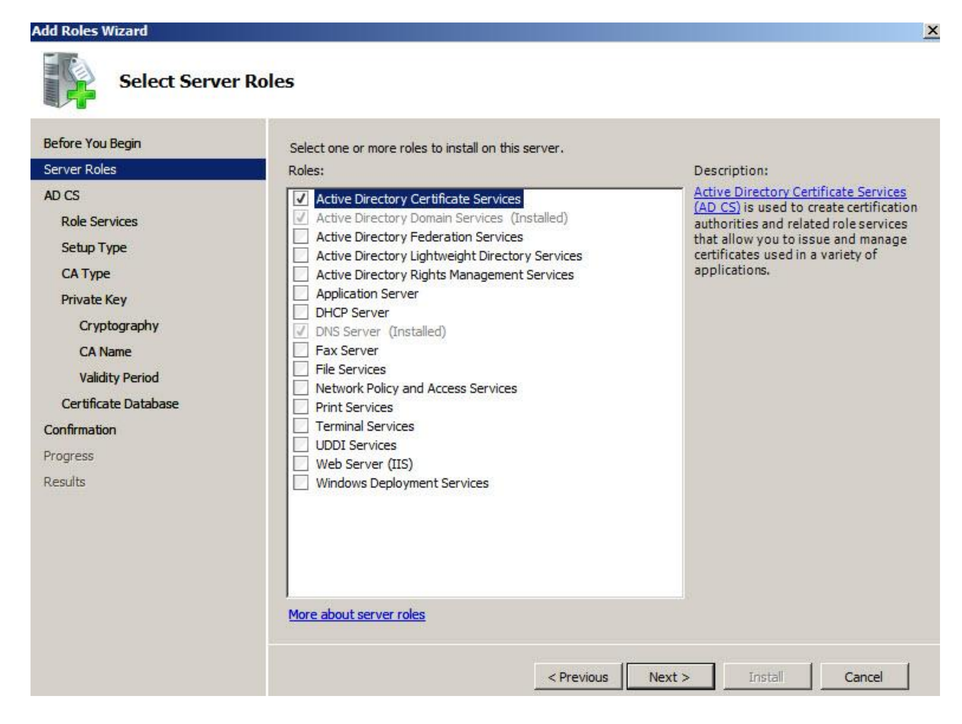
Stores directory data and manages communication between users and domains, including user logon processes, authentication, and directory searches.

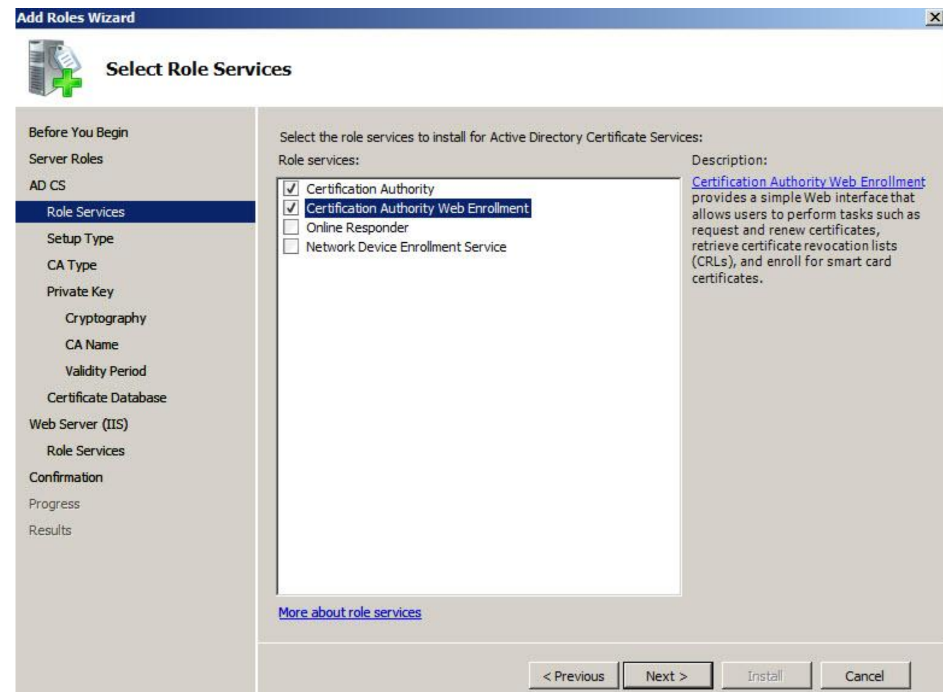
Role Status — Go to Active Directory Domain Services

Messages: None
System Services: 8 Running, 2 Stopped
Events: 2 warnings, 6 informational in the last 24 hours

Last Refresh: 7/30/2012 2:57:56 AM Configure refresh

نختار AD Certification Services





Web Enrollment

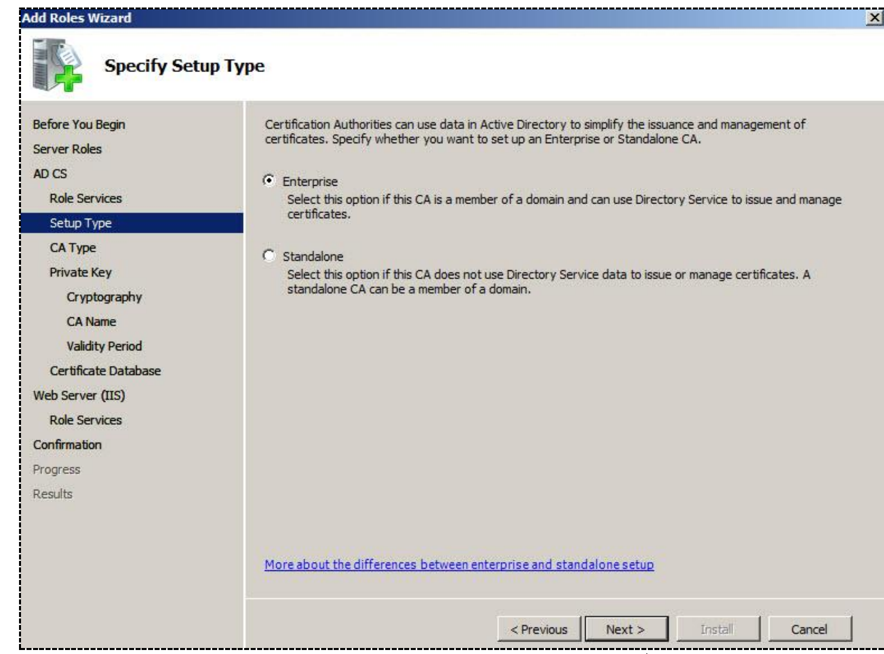
المسئوله عن ان الUser يحصل علي الCertification عن طريق ال Website

Online Responder

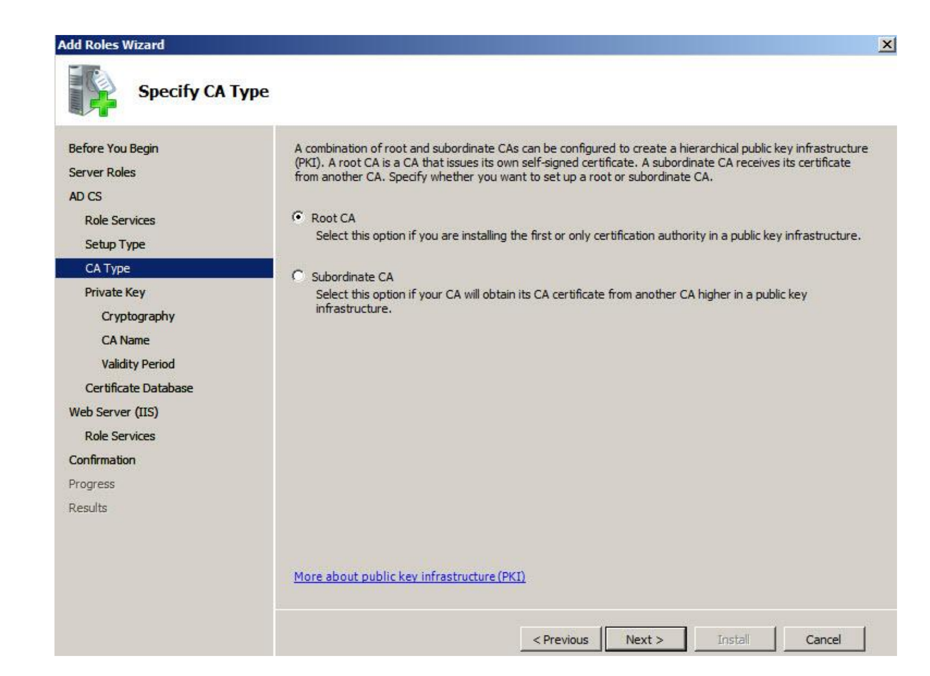
المسئوله عن حفظ ونشر الCertification المرفوضه للتحذير منها (إختياريا)



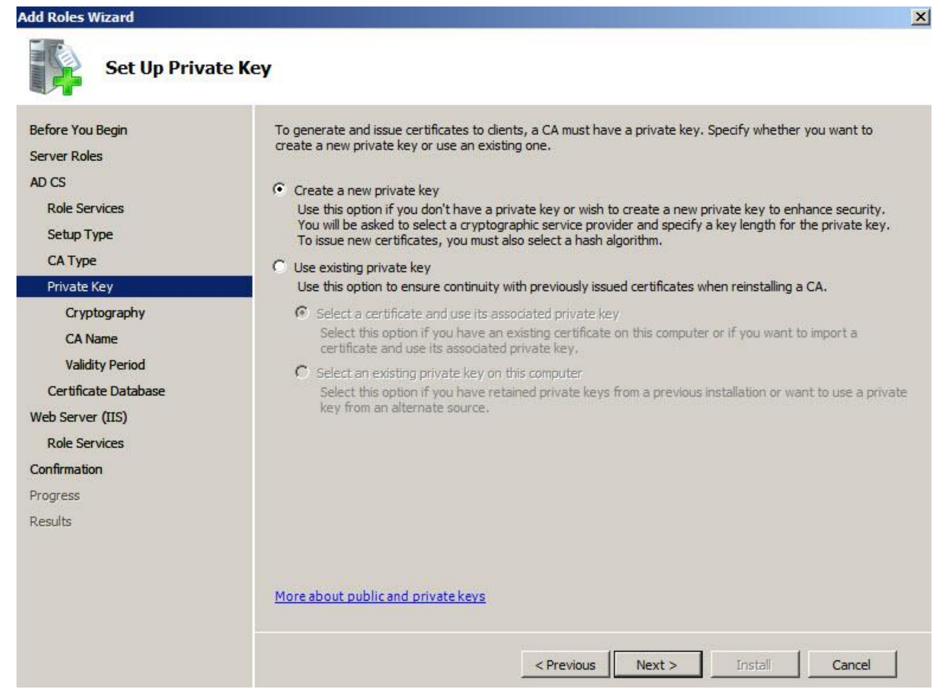
يتم تنزيل خدمه الIIS



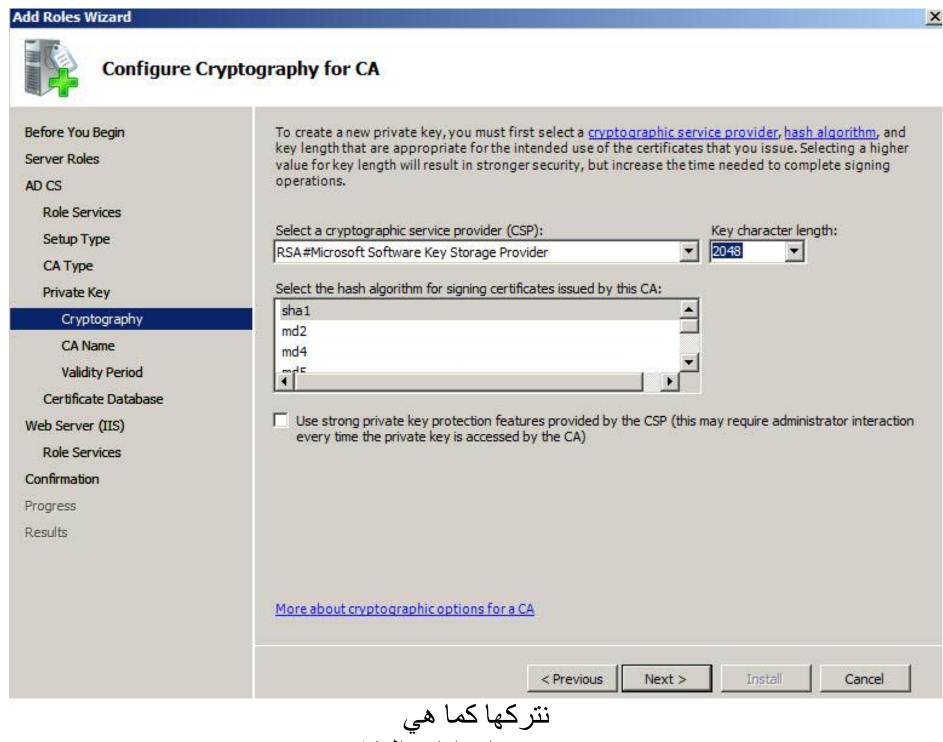
لأن هذا الجهاز Domain Controller ظهرت Enterprise متاحه ونقوم بإختيارها
ولأجل الإستفاده ايضا من الخصائص الموجوده به وهي الWeb Interface والMMC
اما اذا كان غير هذا ستكون فقط الStand alone المتاحه



لأنه هو اول Server يقدم هذه الخدمه حاليا

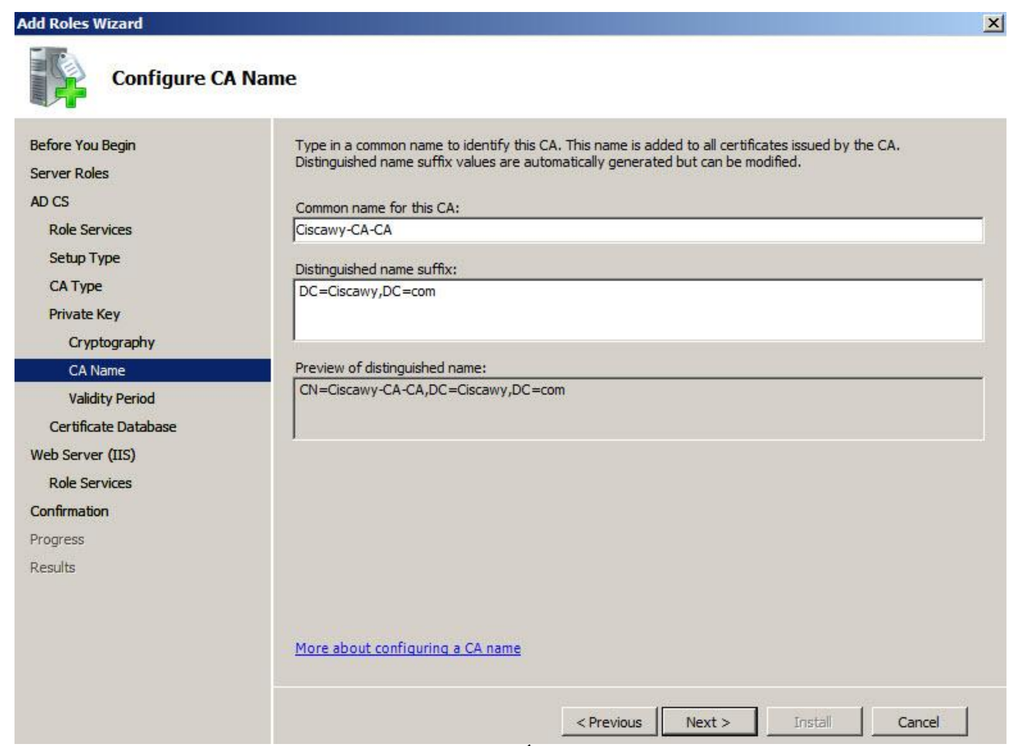


سنقوم بإنشاء Key جديد

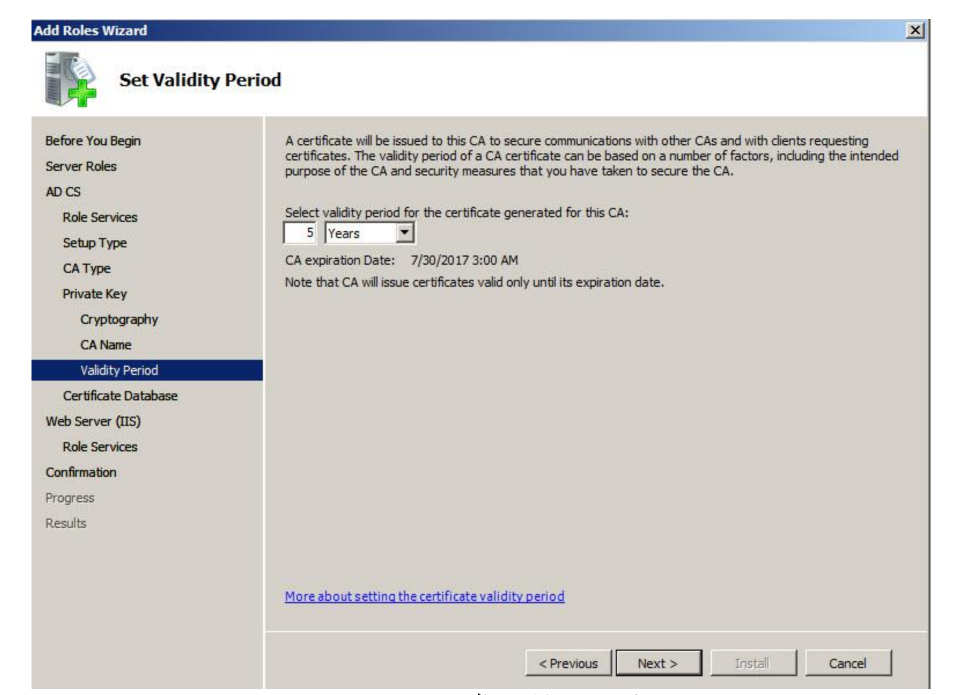


نتركها كما هي

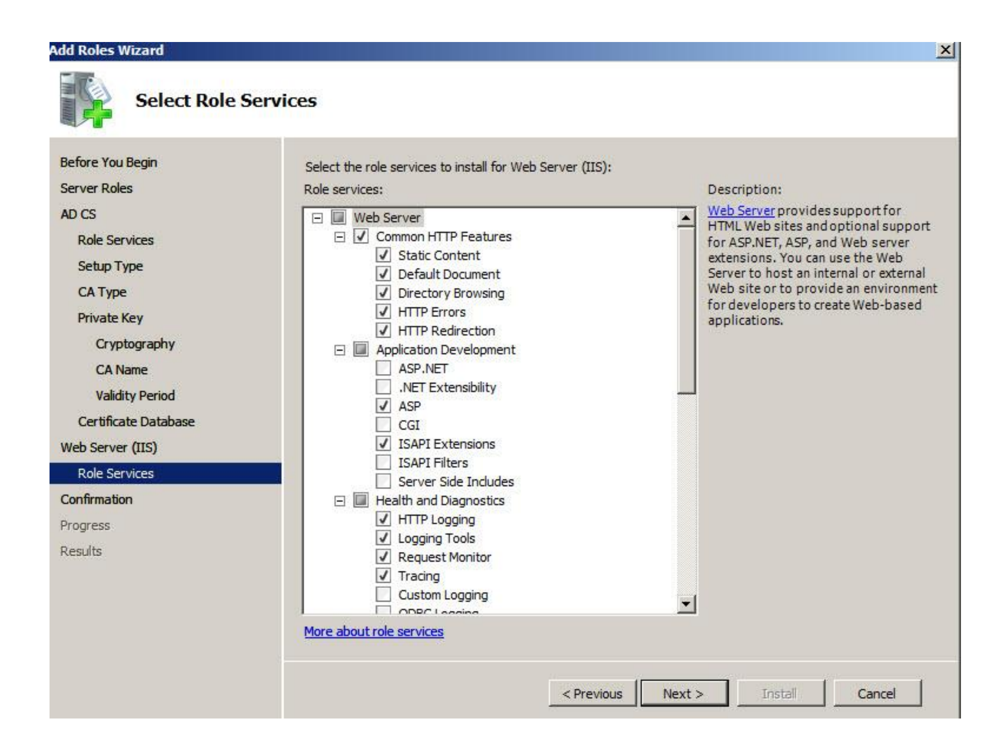
و هي تخص إعدادات التشفير



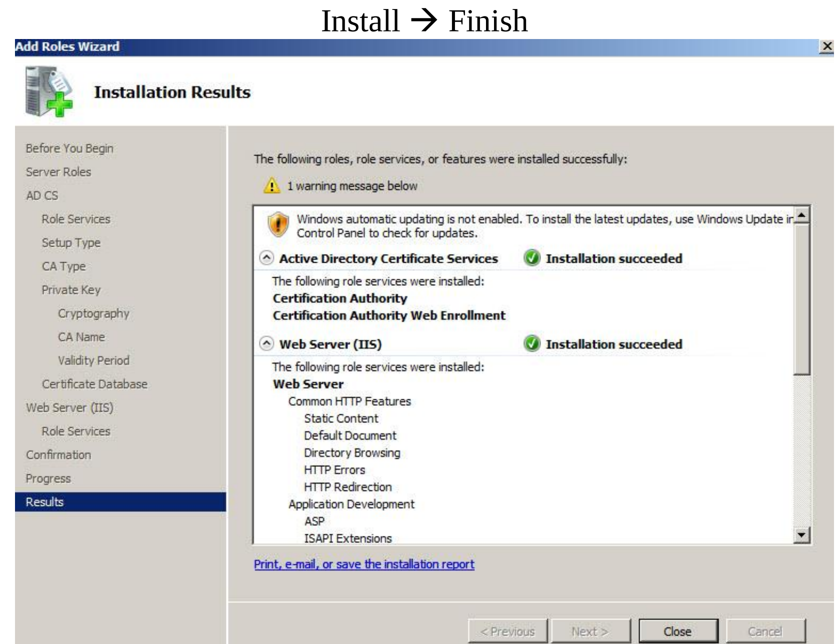
يمكنك ان تقوم بتسميه الMachine من هنا لأن بعد تنزيل هذه الخدمه لن تستطيع اعاده تسميتها الا بعد حزف هذه الخدمه



خاصه بصلاحيه الCertification

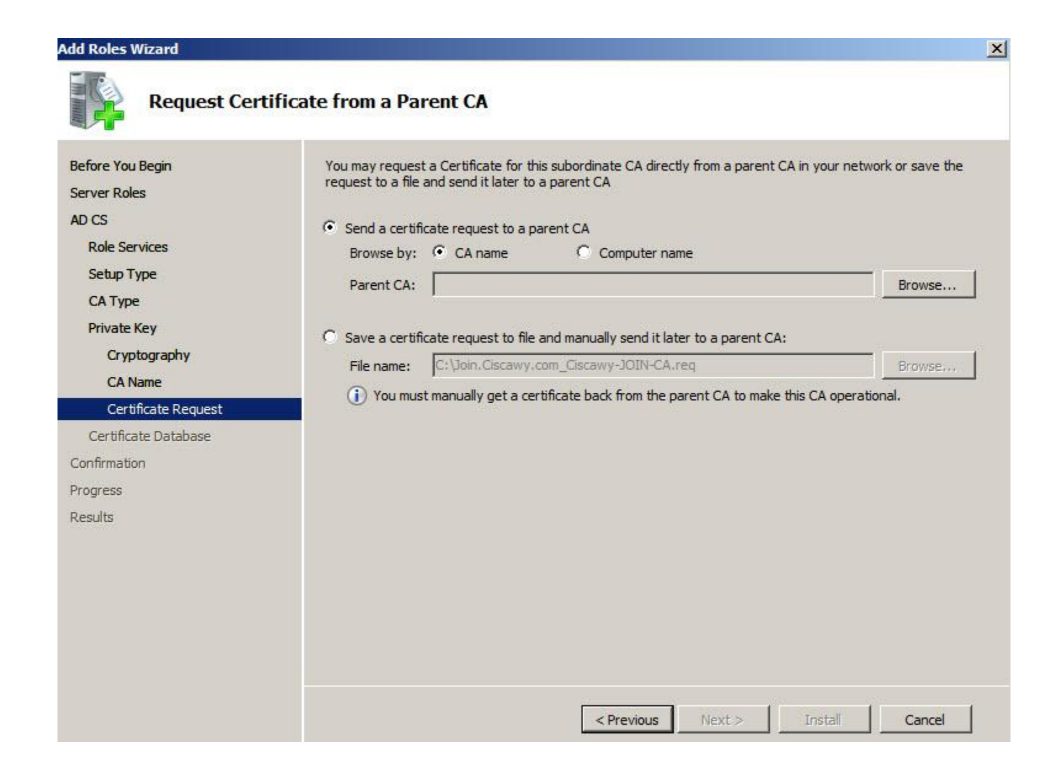


Install → Finish



- بعد الانتهاء من عمليه التصطيب

اذا أردنا بعد ذلك ان نضيف Server اخر يكون Sub-ordinate
لا بد ان تكون الMachine متصلة Joined in Domain
ونقوم بعمل خطوات تنزيل ال CS طبيعي جدا



في هذه الخطوه يطلب الCertificate

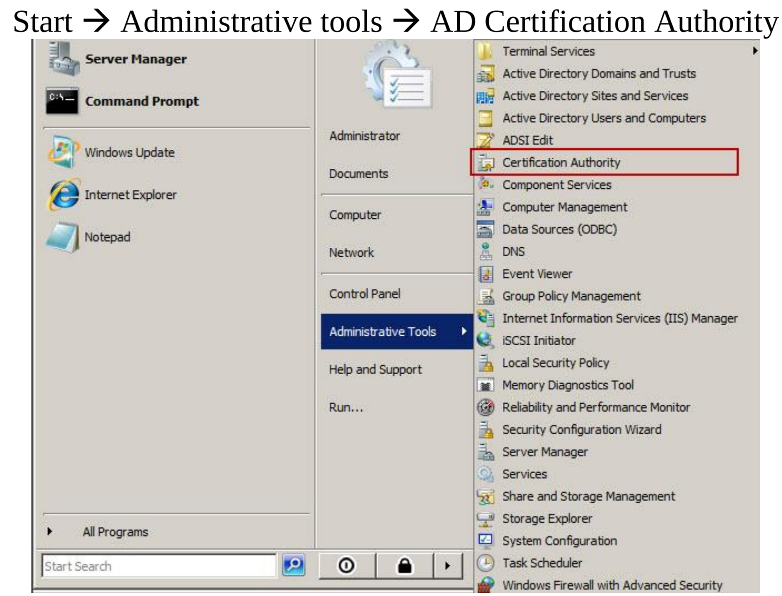
ممكن ان يتم اضافتها اذا كان الRoot يعمل بالضغط علي Browse ونضيفه

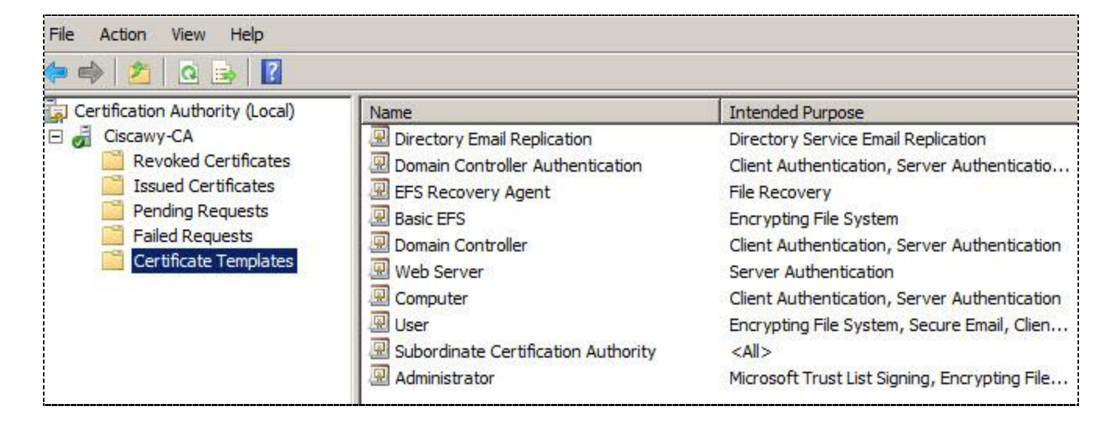


أو يتم حفضها في ملف وسكون وبعد ذلك يقوم الAdministrator بعمل Approve لها

- نقوم بفتح الCA

Start → Administrative tools → AD Certification Authority





- Revoked Certificates

الشهادات المرفوضه او الغير معترف بيها

- Issued Certificates

التي تم طلبها وتسليمها لل Users تلقائيا وسنجد ان هناك Certificate قد حصل عليها الAdministrator حينما اخترانا في التنصيب ان يقوم بإنشاء Self Sign Certificate

- Pending Certificates

الشهادات التي علي الAdministrator ان يقوم بالموافقه عليها او رفضها

.

- Failed Certificates

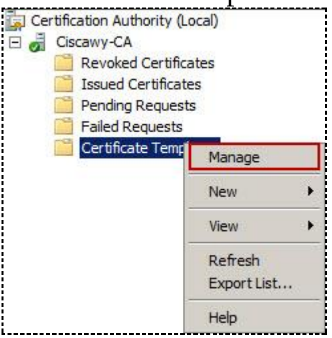
الشهادات المرفوضه من قبل الAdministrator

- Certificate Templates

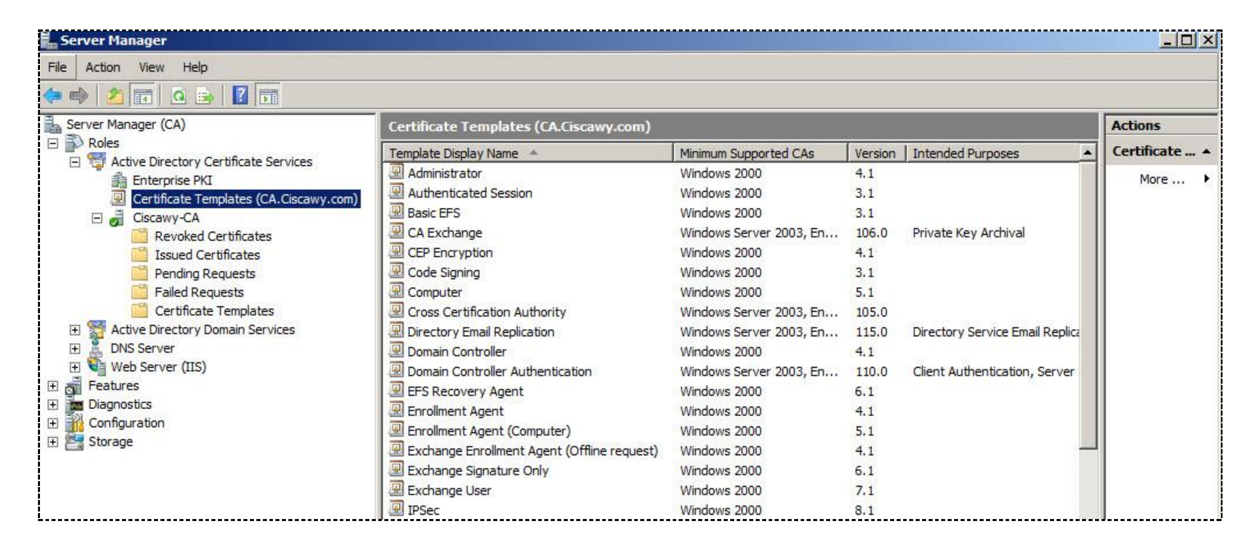
التي يسمح للUsers ان يتعاملوا معها

ولكن اين الTemplates التي يتم التعديل والتعامل معها لتطبيقها علي الUsers ؟!!

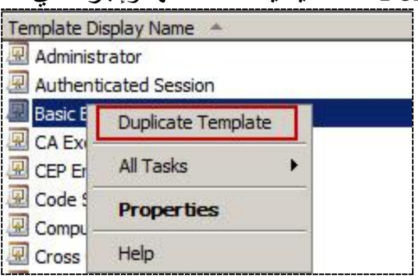
R.click on Certificate Templates →Manage

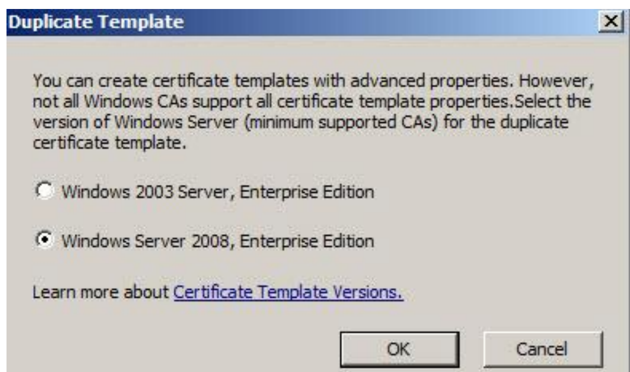


او من عن طريق فتح الServer Manager سنجدها تلقائيا دون الحاجه الي الR.click

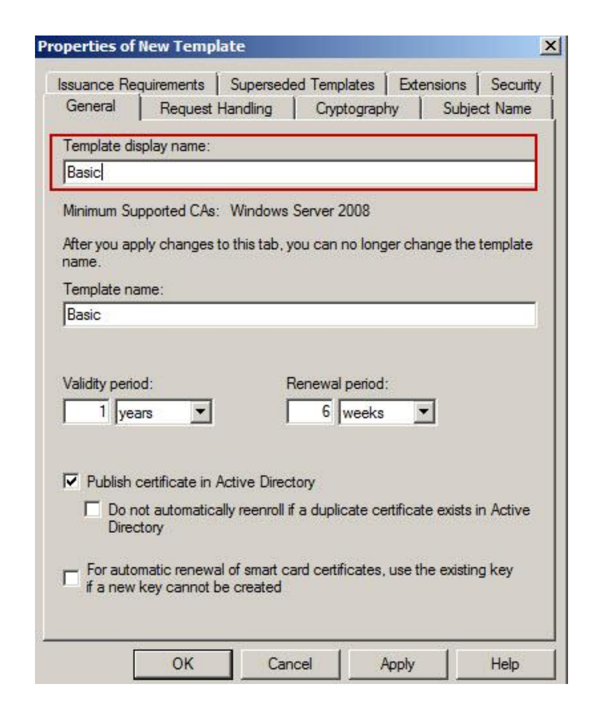


علي أي Template اقوم بالضغط R.click ومنها Duplicate
لأنه لا يسمح لأن يتم التغيير في الPolicies الاساسيه يمكنك نسخها وإجراء اي تعديل تبغاه



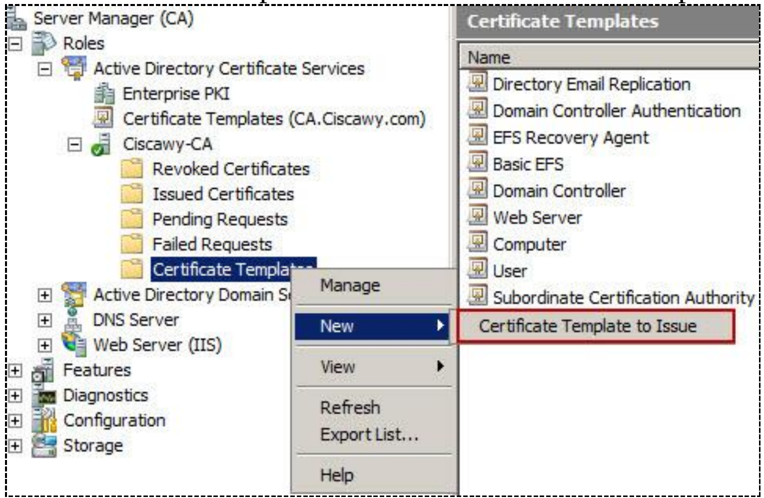


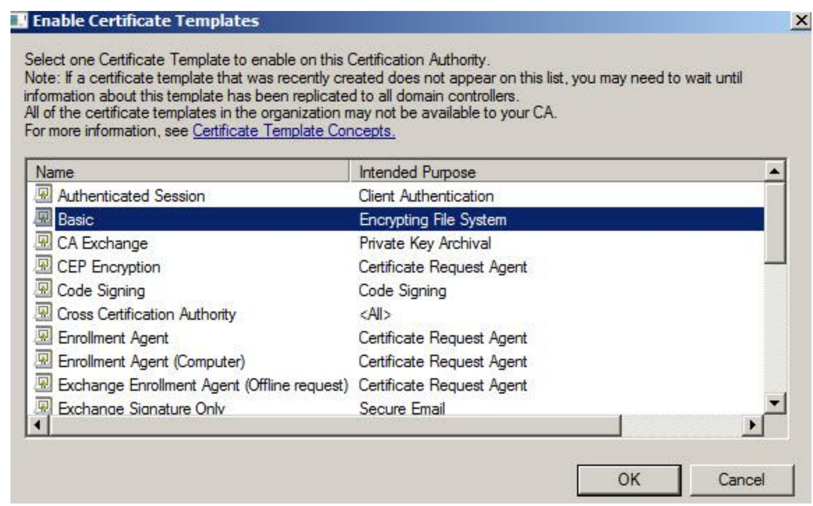
يمكنك تغيير اي شئ تريده
وتغيير ايضا الصلاحيه الخاصه بهذه ال Template



يعد الضغط علي OK ستجد انه لم يتم نشرها Enrollment !!

R.click on Certificate Template → New → Certificate Template to Issue





نقوم بإختيارها ونضغط علي OK

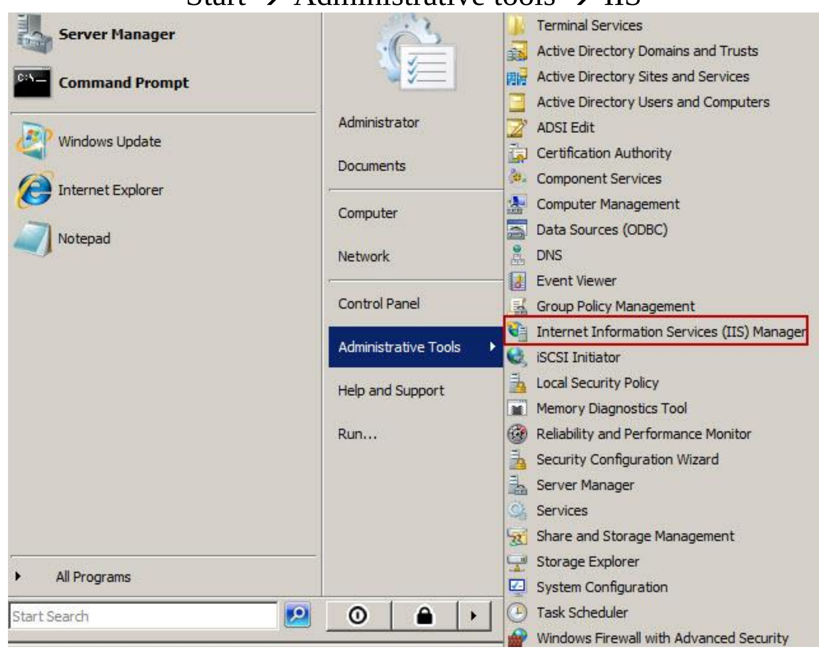
سنجد انها تم ادراجها في الCertificate Template

يحصل الUser علي الCertificate عن طريق

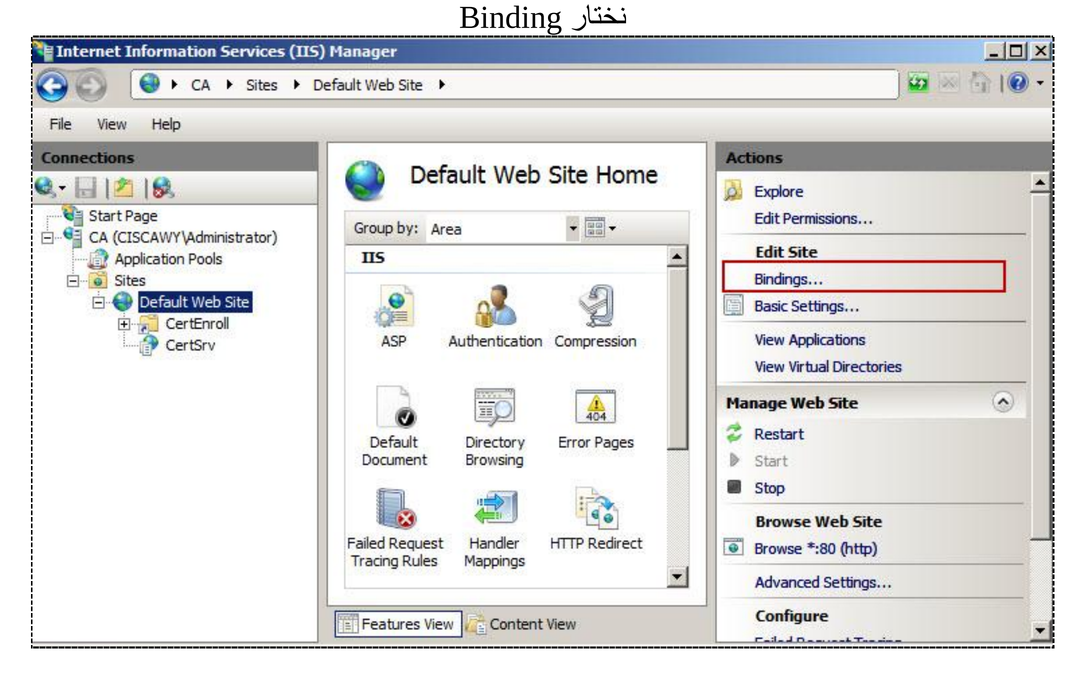
- Web Server
- MMC
- Group Policy تأخذ فقط الCert المفعل عليها خاصتي الEnroll & Autoenroll

• نقوم بفتح الIIS لأعداه

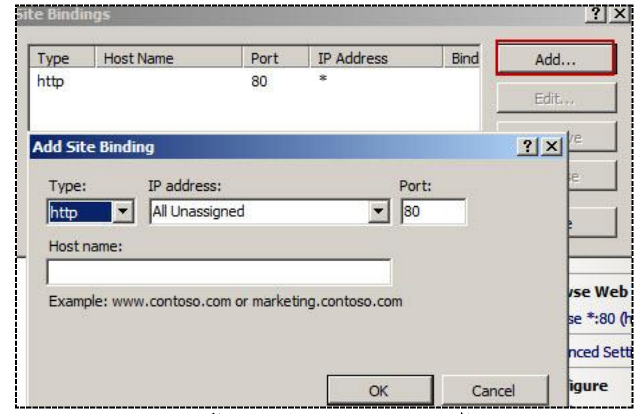
Start → Administrative tools → IIS



يستخدم الIIS تلقائيا الHTTP في الدخول عليه
ولكن هذا Not Secure لذا يجب ان نضيف استخدام الHTTPS
نختار Binding



ونقوم بالضغط علي Add



ونضيف الHTTPS ونختار اسم الMachine

سمحت انه يستخدم الHTTPS في عمليه الConnection



يمكن ان نقوم بالضغط علي View لقراءة الCertificate التي حصل عليها الDomain



نقوم بفتح الInternet Explorer ونكتب عنوان ال Web Server
https:\\ca.ciscawy.com\certsrv
ca.ciscawy.com اسم الجهاز

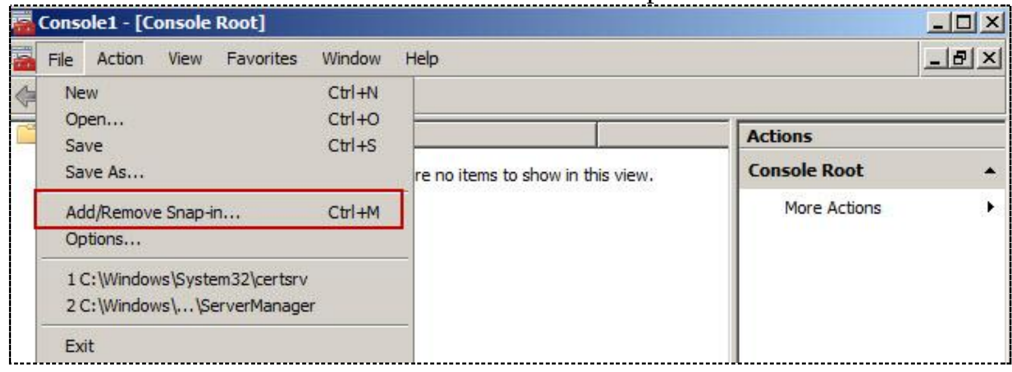
سنجد انه يطلب الCredential الخاصه بالUser



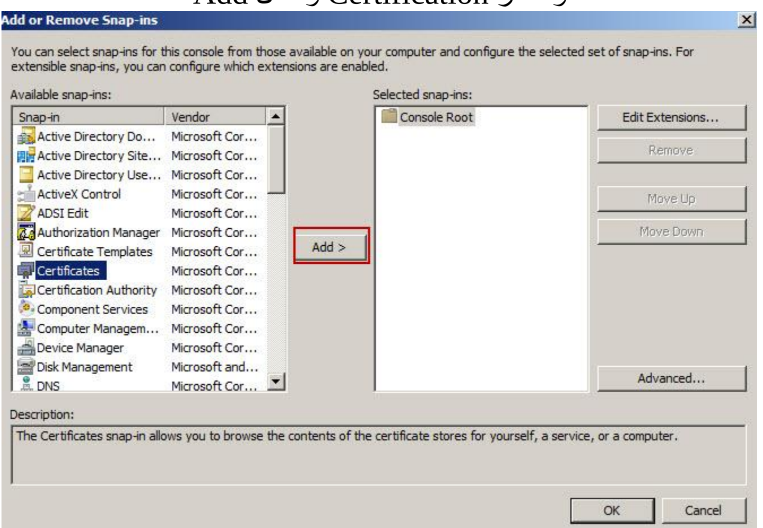
للتأكد من ان الCA الخاص بي أصبح معتمدا ويعمل بطريقه صحيحه !!

Run → MMC

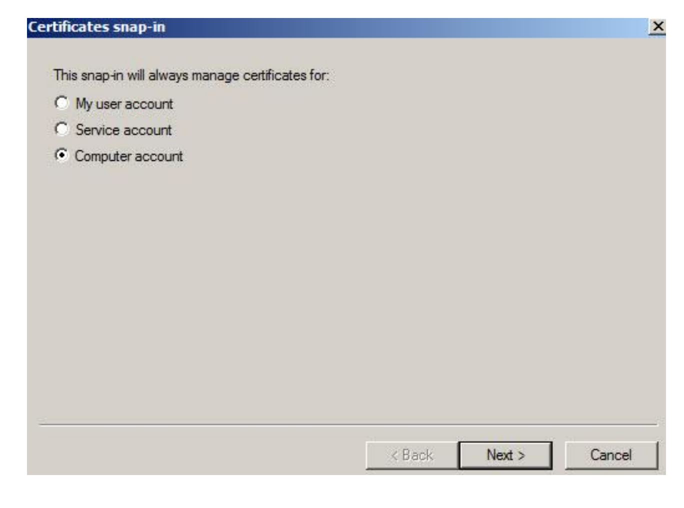
File → Add/Remove Snap-in

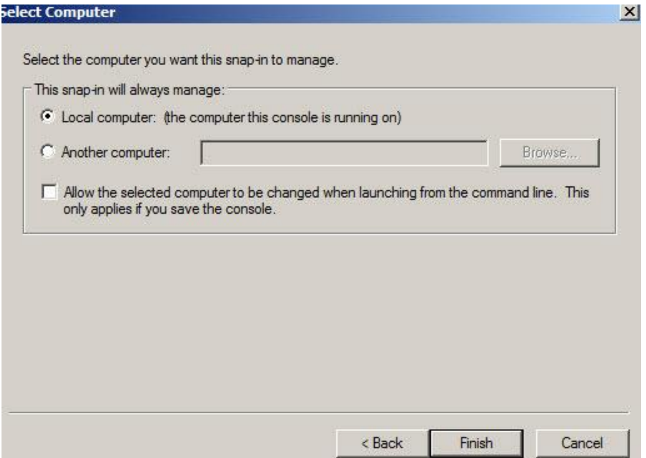


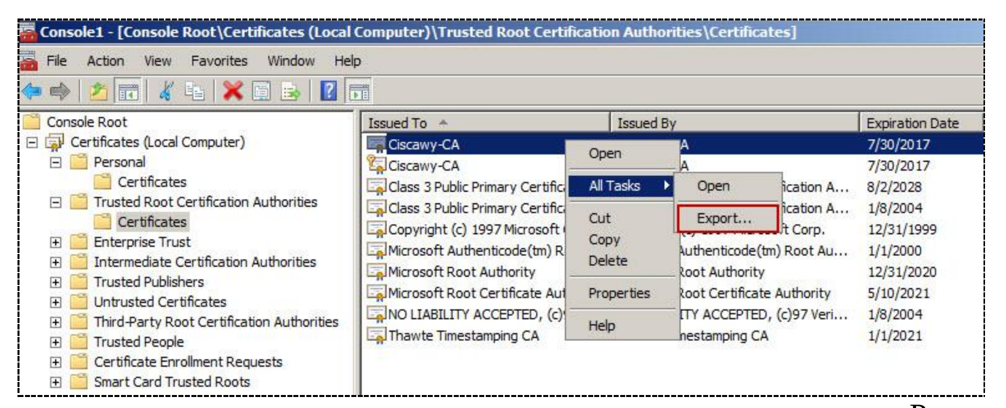
ونختار Certification ونعمل Add



نختار Computer Account







- Personal

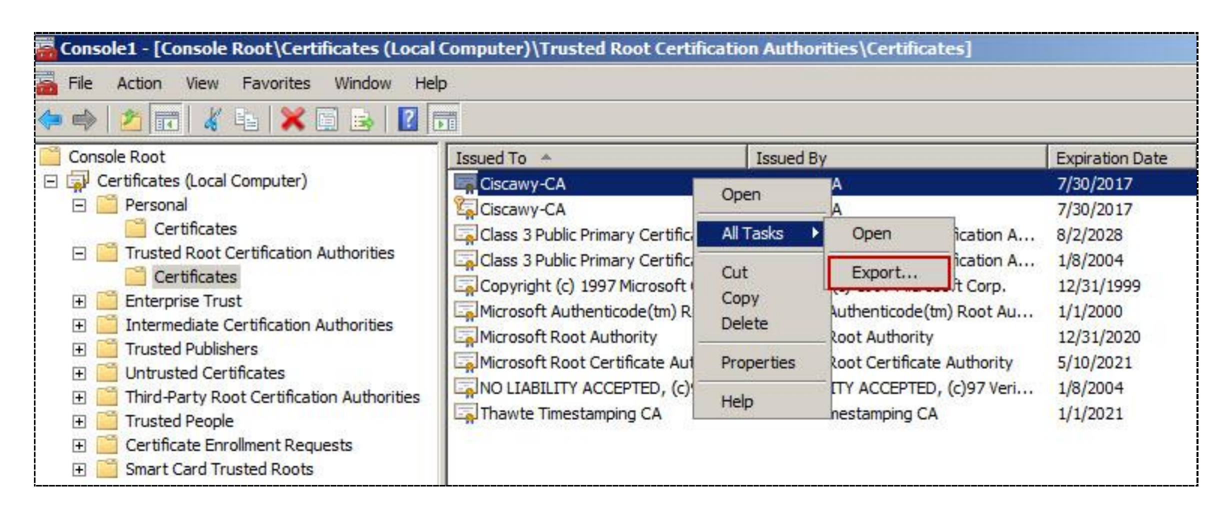
ال Certification اللي حصل عليها اي User

- Trusted

توضح عناوين الServers الموثوق فيها وبعد كدا ممكن نتأكد من تاريخ صلاحيتها واسم الSite المرسله منه

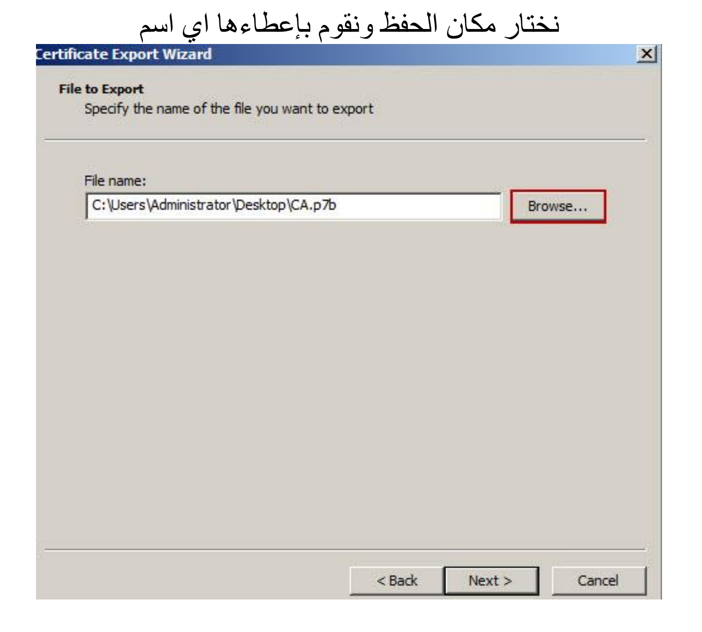
لعمل Export لأي Certification حتي نقوم بإستخدامها مع أي User

R.click علي اي منهما ونختار All Tasks → Export





نختار مكان الحفظ ونقوم بإعطاءها اي اسم

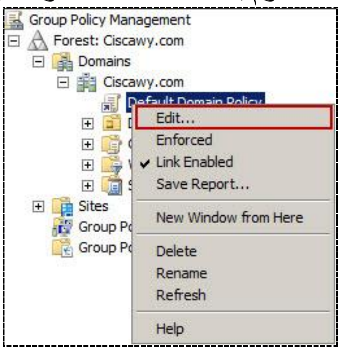


نضغط علي Next → Finish

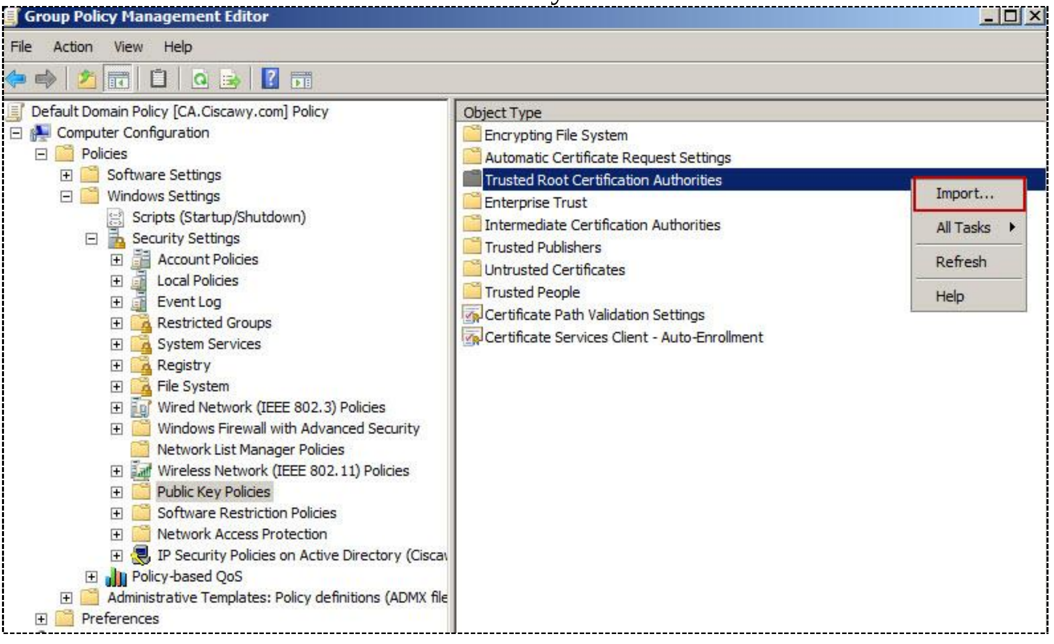


لكي نقوم بتطبيق هذه الCertification علي كل الUsers ويستخدموها وتكون بالنسبه لهم Trusted Root ويضاف داخل قائمة الTrusted :-

نقوم بفتح الGroup Policy و علي الDefault نقوم بالضغط R.click ونختار Edit



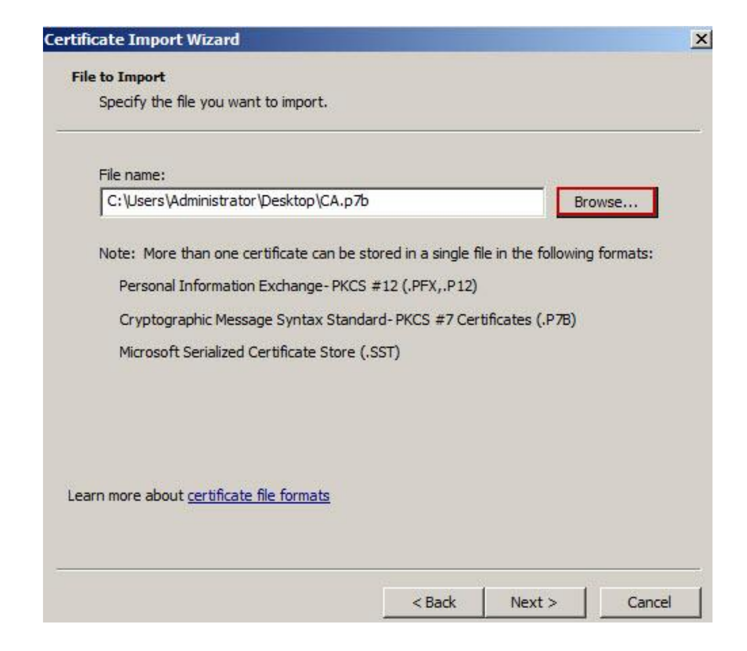
Computer Configuration → Policies → Windows Setting → Security Settings → Public Key Policy



نضغط R.click علي الTrusted Root ونختار Import

Next

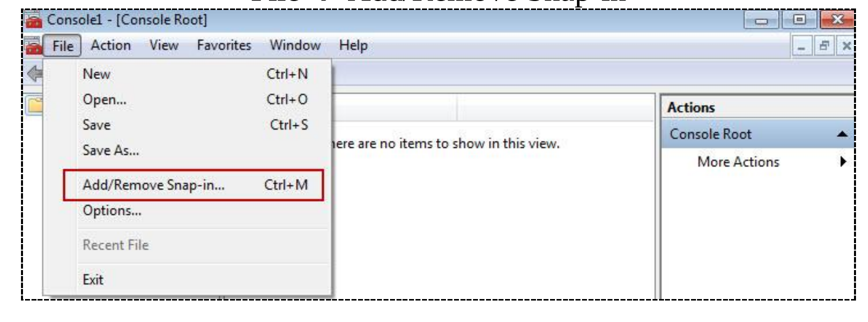
نختار الCertification



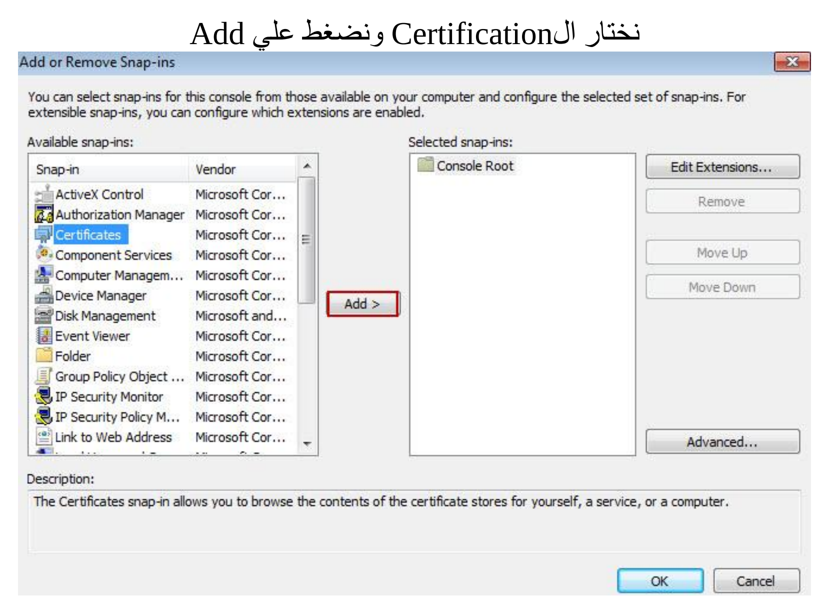
Next → Finish

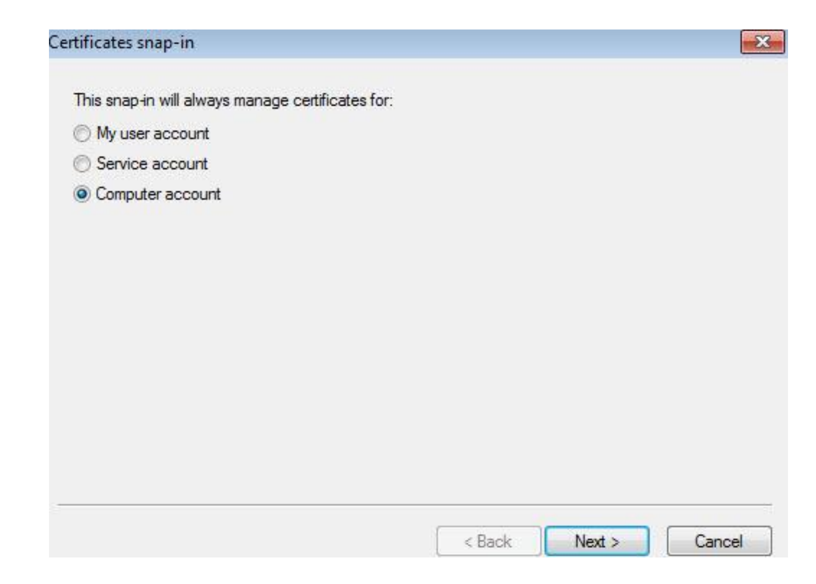
علي جهاز الـWin-7
نقوم بفتح الـInternet Explorer ونكتب عنوان الـ Web Server
https:\\ca.ciscawy.com\certsrv
ستجد انه يعطيك رساله تحزيريه تفيد بأن هذا الـSite غير موثوق فيه

نقوم بفتح Run → MMC
File → Add/Remove Snap-in

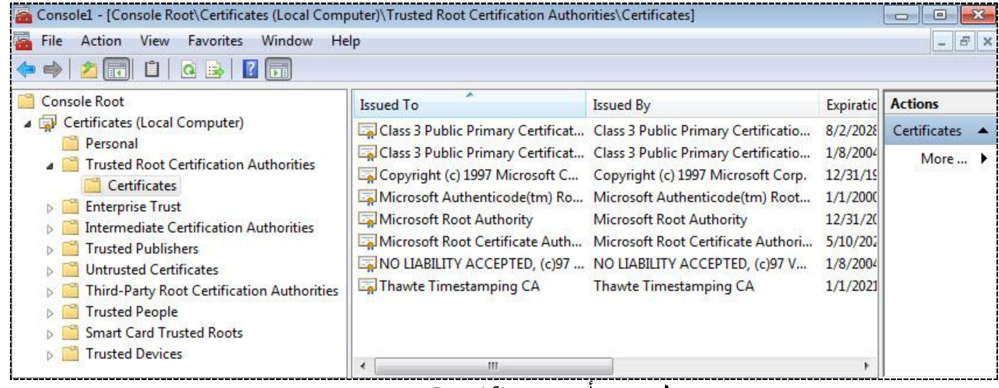


نختار الـCertification ونضغط علي Add



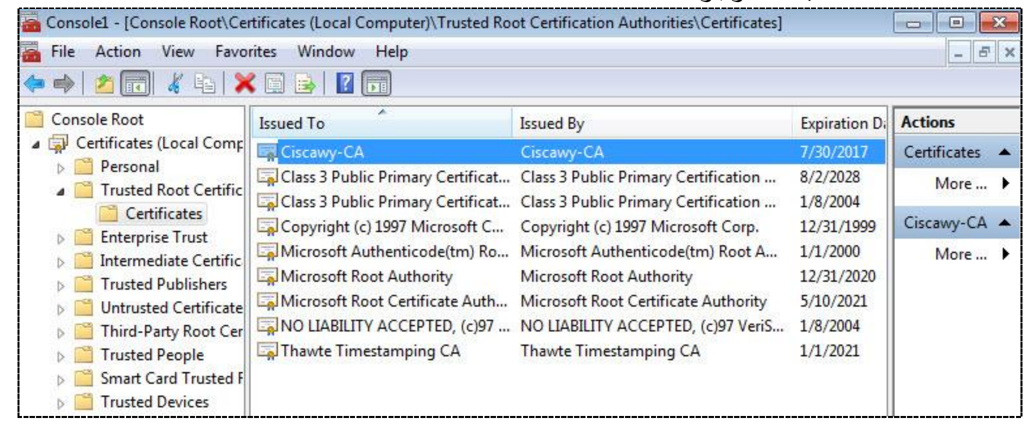


نختار Computer Account
Next → Finish

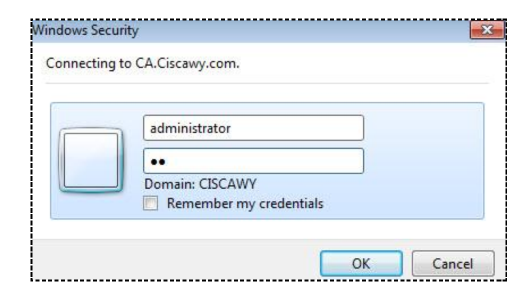


لن نجد أي Certificate موجوده

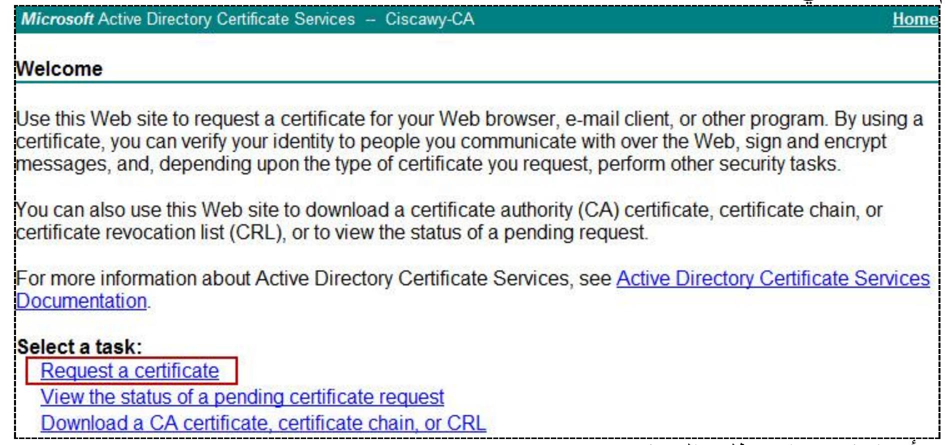
نقوم بعمل Restart للجهاز مع تفعيل الGroup Policy واعاده نفس الخطوات
سنلاحظ انه الCertificate اصبحت موجوده



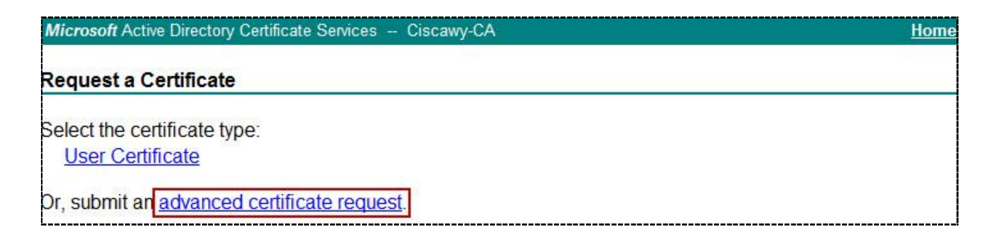
وعند فتح الInternet Explorer ونكتب عنوان ال Web Server
https:\\ca.ciscawy.com\certsrv
سيقوم بسؤالك عن الCredential الخاصه بالمستخدم



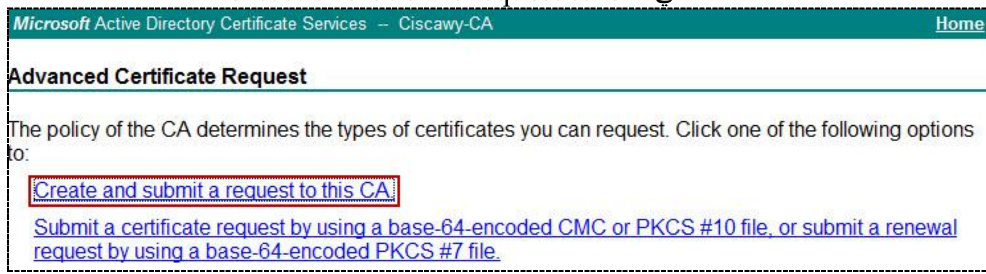
- سنقوم بالدخول علي الWeb Server



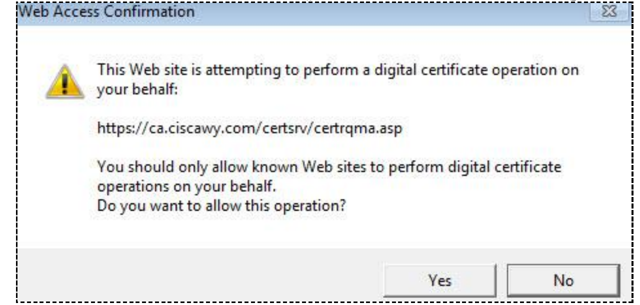
نختار Request أي اننا نريد ان نطلب الشهاده

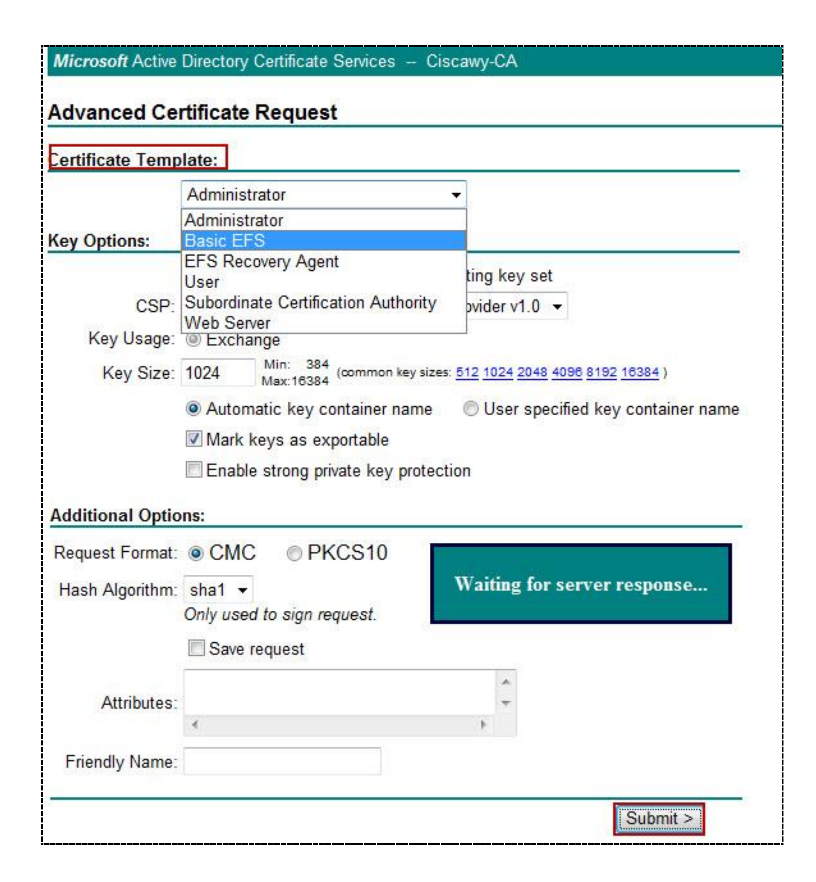


نضغط علي Create and Submit request to CA

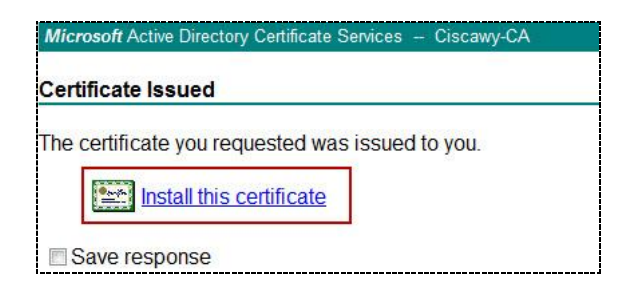


رساله توضح اننا بالفعل متاوجدون علي الServer و هو يقدم خدمه الCA

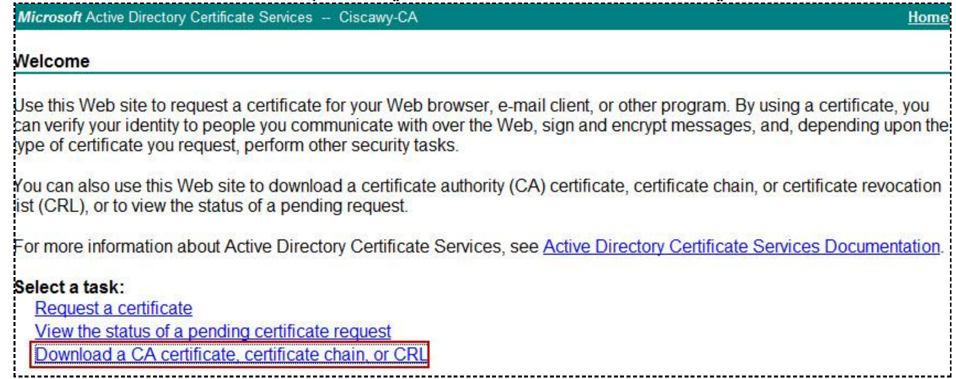


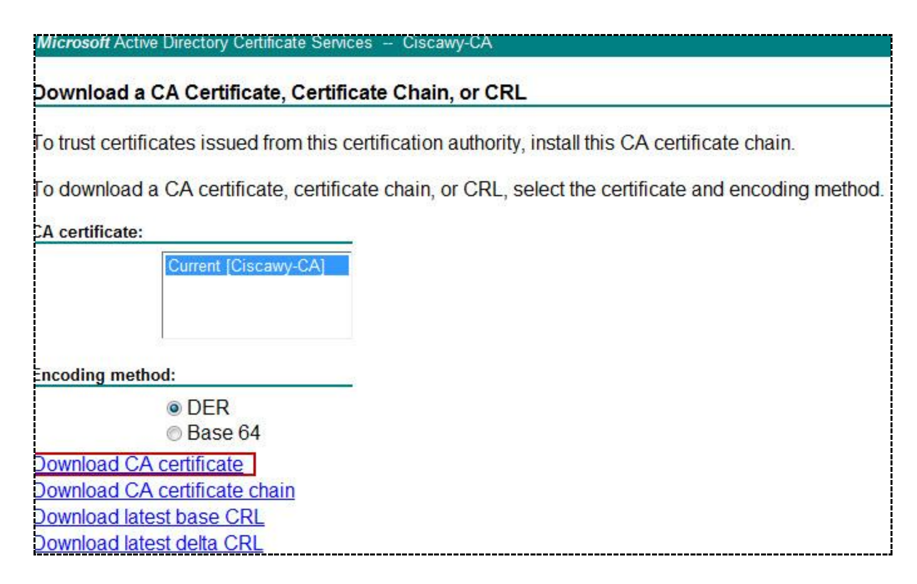


نختار النوع ونقوم بالضغط علي Submit
ستظهر رساله تفيد ان تمت عمليه التصطيب بنجاح



يمكن ان نقوم بإختيار Download في حالة إذا اردت الاحتفاظ بها علي جهازي



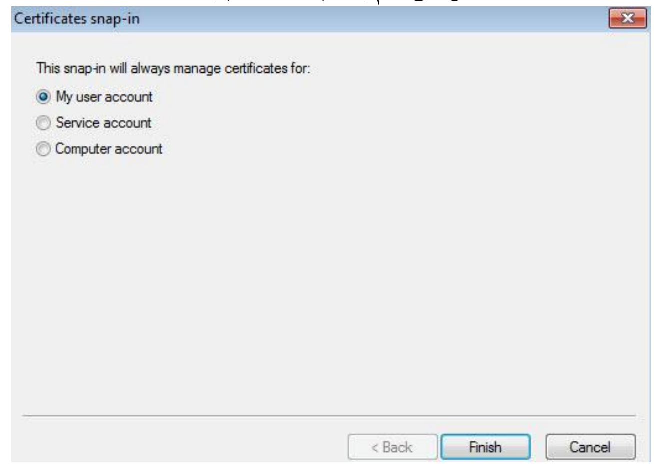




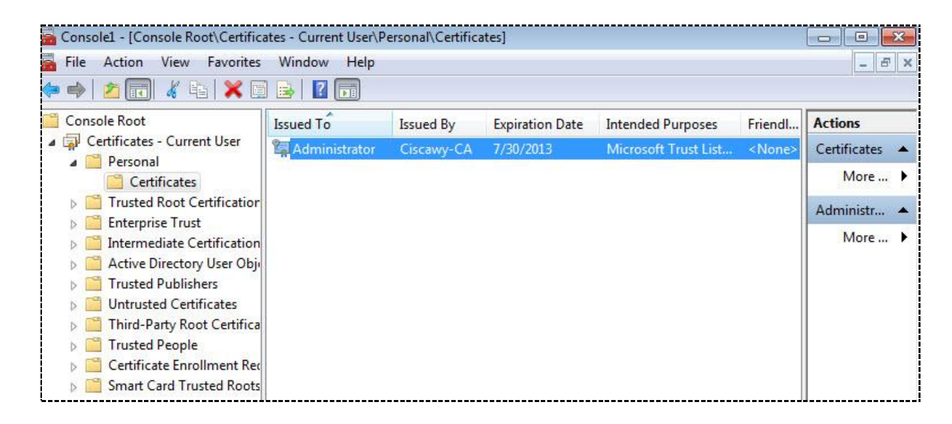
ثم نضغط علي Save لحفظها

- نقوم بفتح الMMC كما في الخطوات التي قمنا بها من قبل

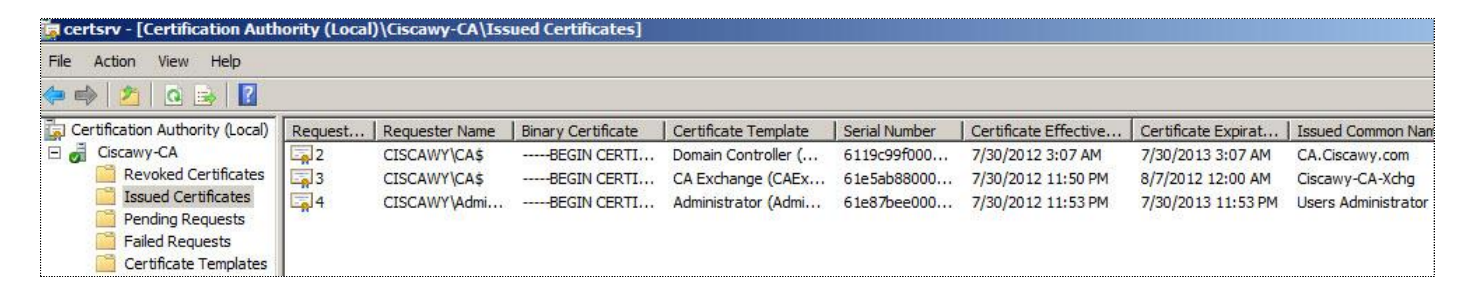
ولكن هذه المره سنختار User Account لأنه هو من قام بعمليه التصطيب



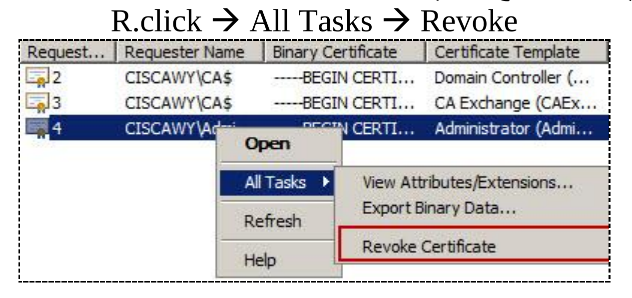
وسنجد أنه تم اضافتها



علي جهاز الServer الذي يلعب دور الCA
نقوم بفتح الIssued Certificate
سنجد انه تم اضافه واحده اخري
٢ تفيد انه هو الDomain Controller
٣ تفيد انه هو الCA
٤ التي طلبها الUser

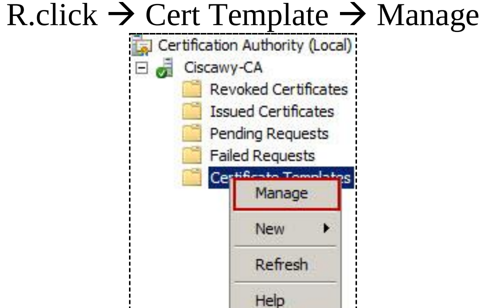


ممكن اعمل Revoke علي أي Cert وامنع ان أي حد يستخدمها
R.click → All Tasks → Revoke

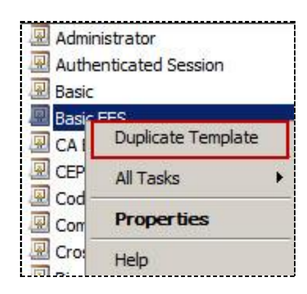


- نقوم بإنشاء User Account جديد

بعد ذلك نقوم بفتح الCertification Authority
R.click → Cert Template → Manage



علي اي Cert نضغط R.click ونختار Duplicate



نضيف لها أي اسم

Properties of New Template

Issuance Requirements | Superseded Templates | Extensions | Security
General | Request Handling | Cryptography | Subject Name

Template display name:
Ahmed-crt

Minimum Supported CAs: Windows Server 2008

After you apply changes to this tab, you can no longer change the template name.

Template name:
Ahmed-crt

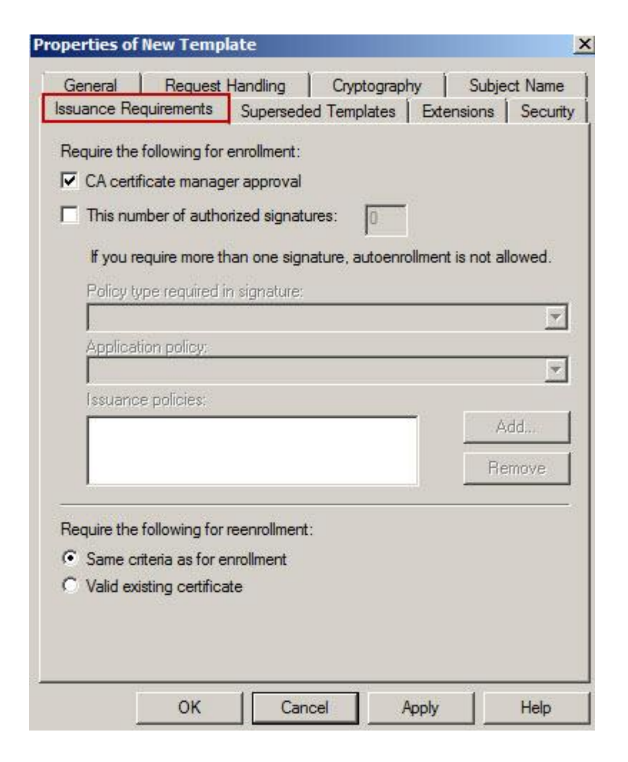
Validity period: 1 years
Renewal period: 6 weeks

Publish certificate in Active Directory
Do not automatically reenroll if a duplicate certificate exists in Active Directory

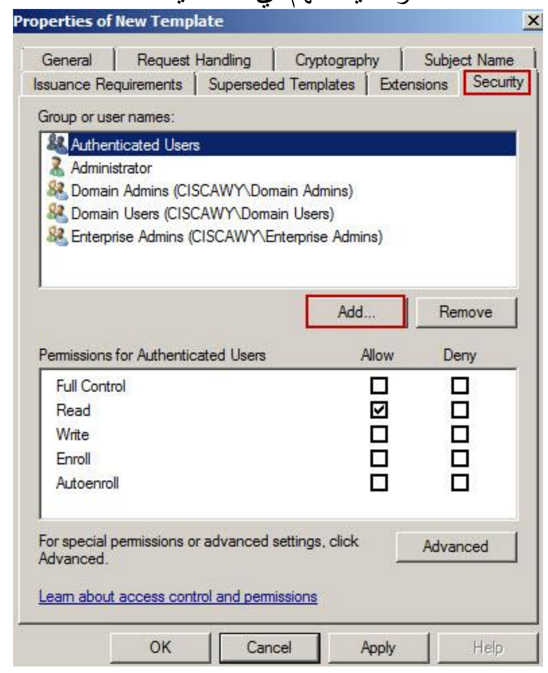
For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

OK Cancel Apply Help

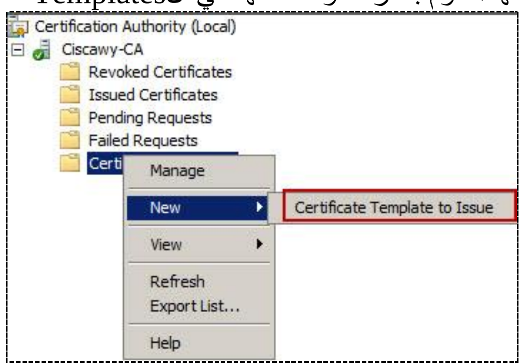
نختار Issuance Requirements
حتي تضيف انه يجب علي الAdministrator السماح بالCert قبل استخدامها

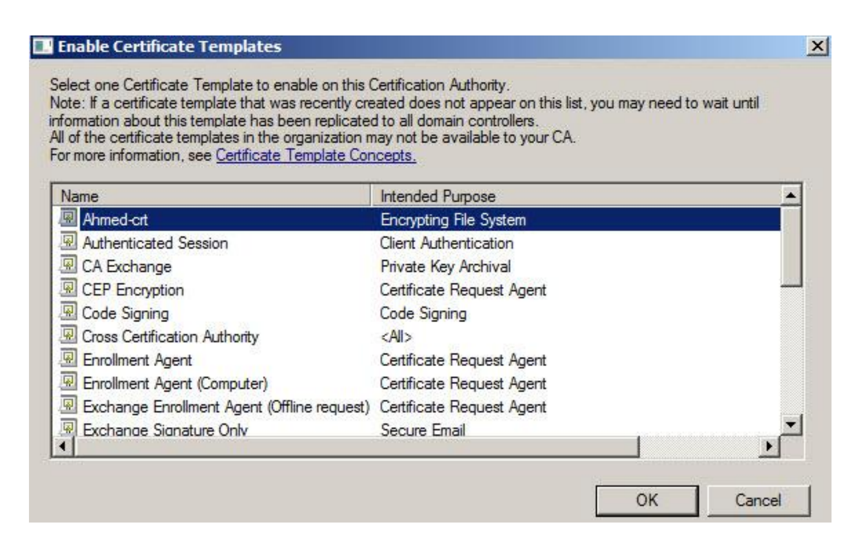


نختار الSecurity
ومن هنا يمكن اضافه الUsers او ال Computers الذين يحق لهم استخدام هذه الCert
وأضيف لهم اي صلاحيات



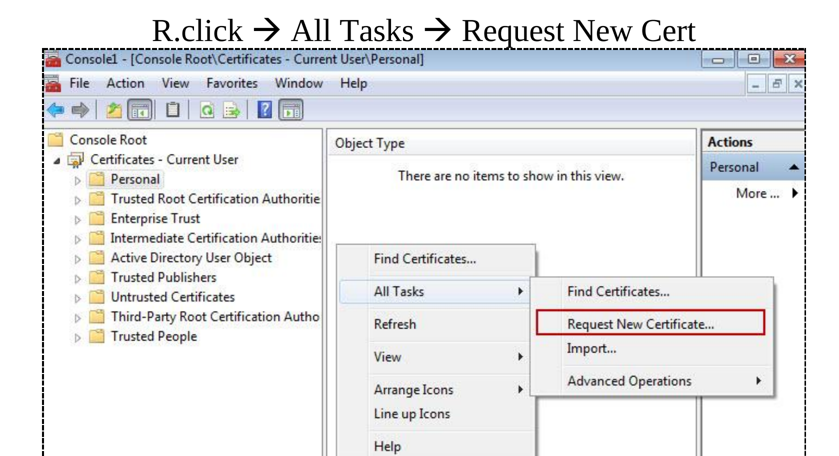
بعد الانتهاء نقوم بنشرها او اضافتها الي الTemplates الموجوده

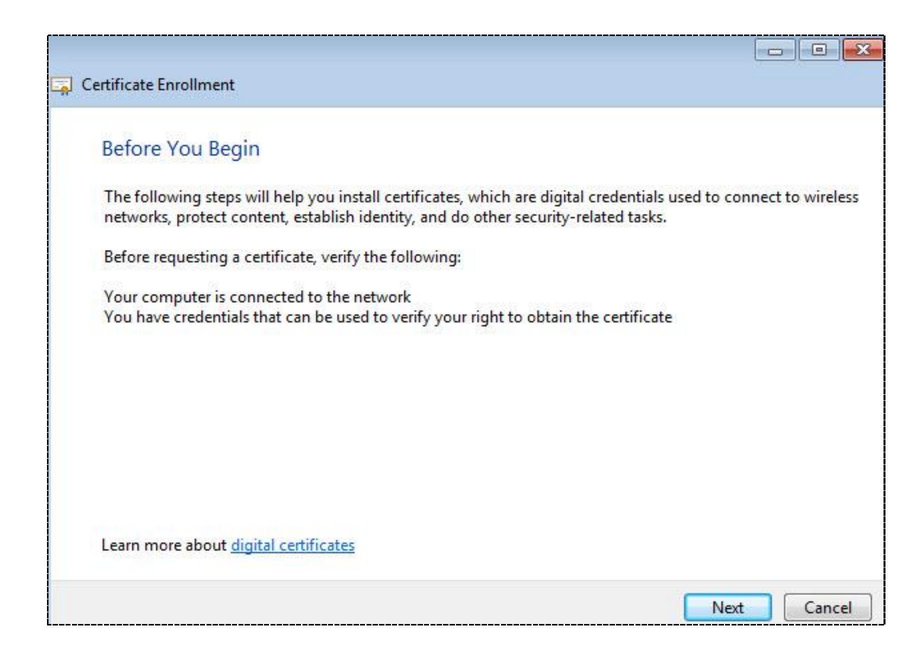




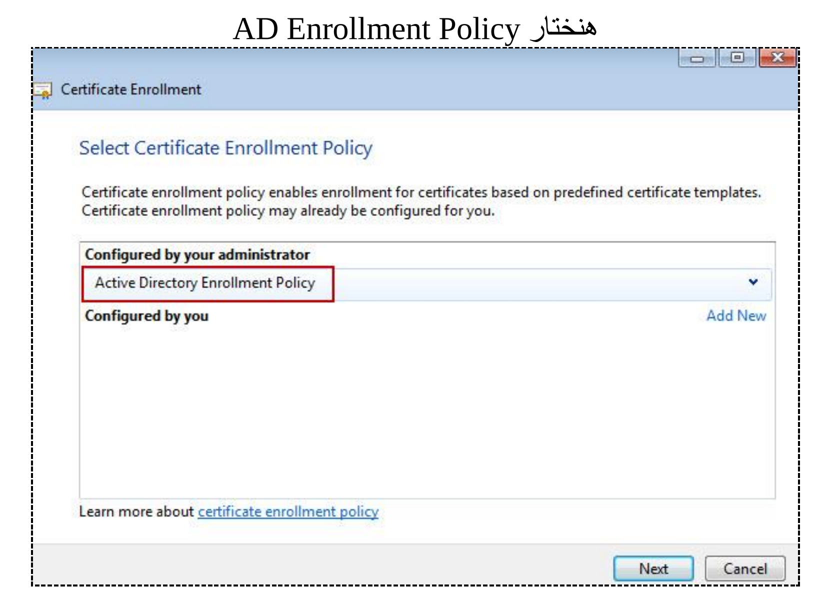
علي جهاز ال7-Win
نقوم بالدخول بصلاحيات الUser الذي تم انشاءه
ونقوم بفتح الMMC الخاص بال Certification كما فعلنا من قبل

R.click → All Tasks → Request New Cert

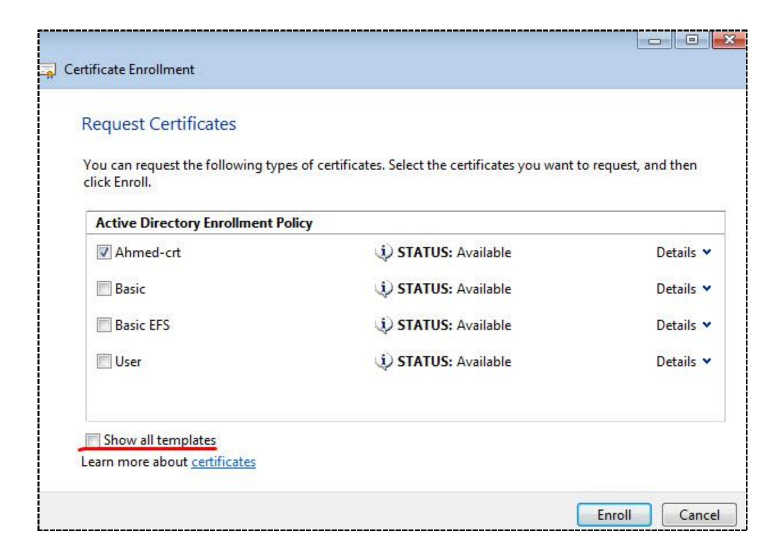


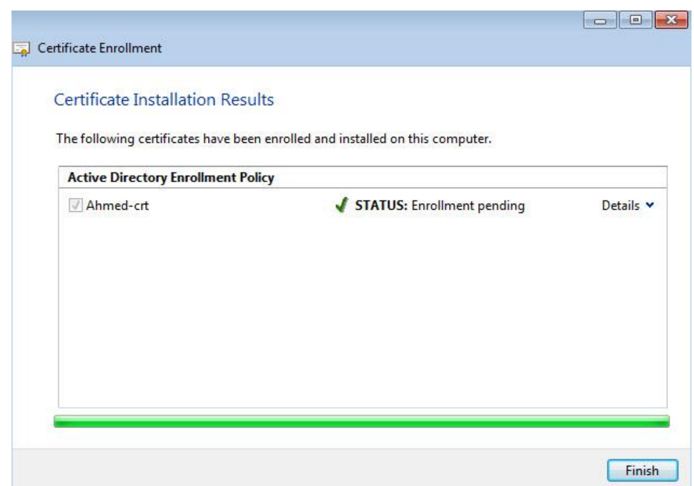


هنختار AD Enrollment Policy



نختار الCert المضافه موخرا
ويمكنك ان تري كل ال المضافه موخرا
ويمكنك ان تري كل الCert عند وضع ✓ علي Show all templates

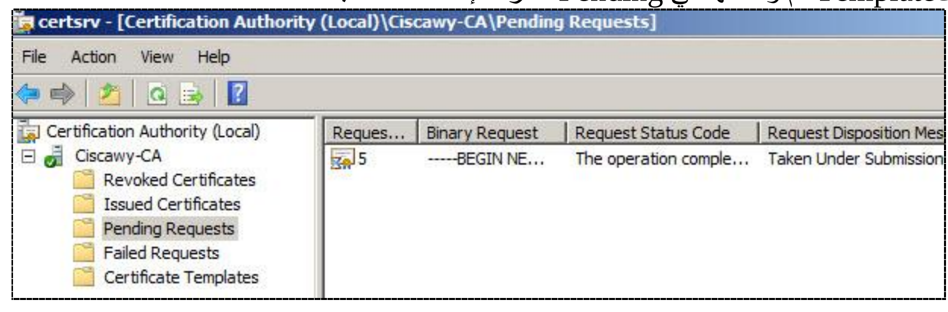




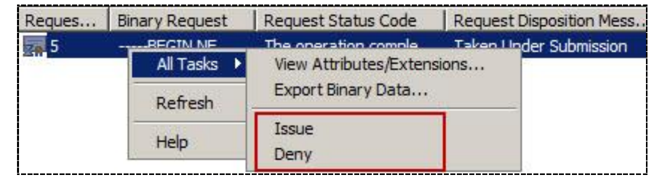
لم يتم اضافه اي شئ في ال Personal !!

علي جهاز الServer

سنجد ان هذه الTemplate تم وضعها في Pending نظرا للإعدادات السابقه



R.click on it → Issue

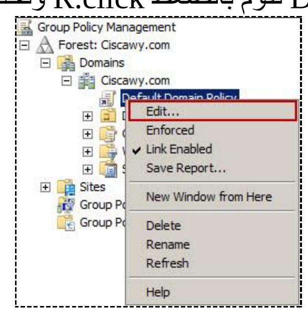


سنقوم بإعاده الدخول مره اخري علي Windows 7

وسنجد انه تم اضافتها بنجاح

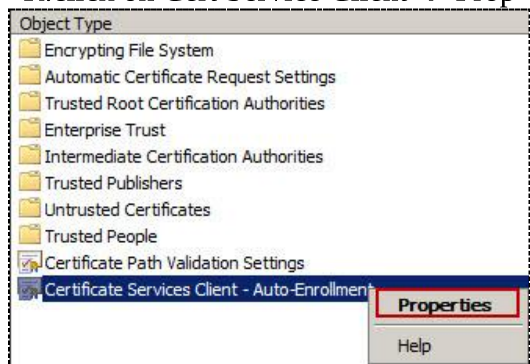
استخدام الGroup Policy في عمل نشر للPolicies

نقوم بفتح الGroup Policy و علي الDefault نقوم بالضغط R.click ونختار Edit

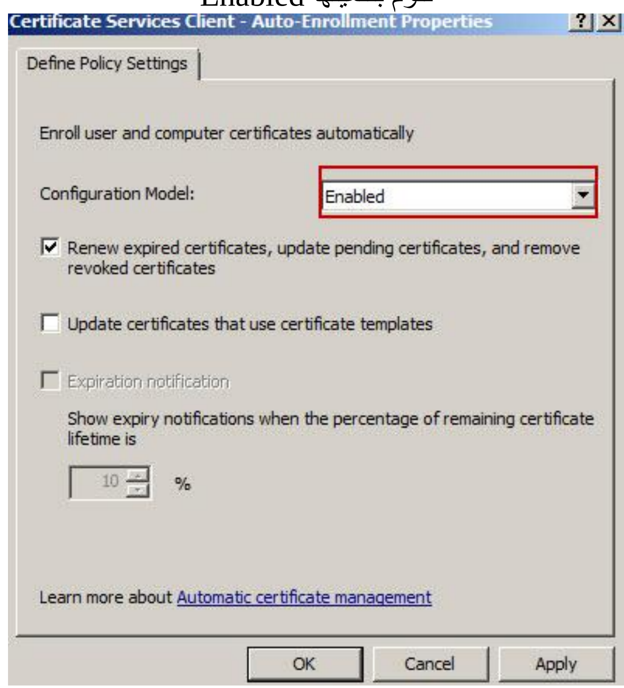


Computer Configuration → Policies → Windows Setting → Security Settings → Public Key Policy

R.click on Cert Service Client → Prop

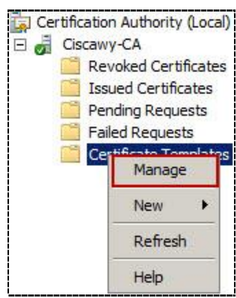


نقوم بتفعيلها Enabled

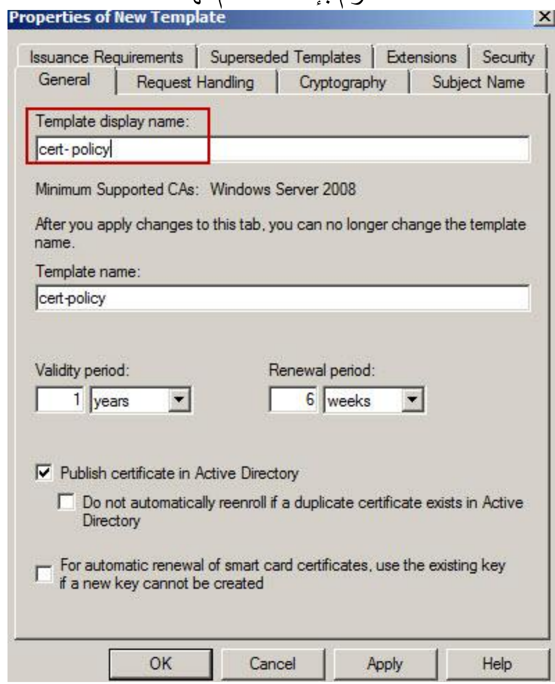


بعد ذلك نقوم بفتح الCertification Authority

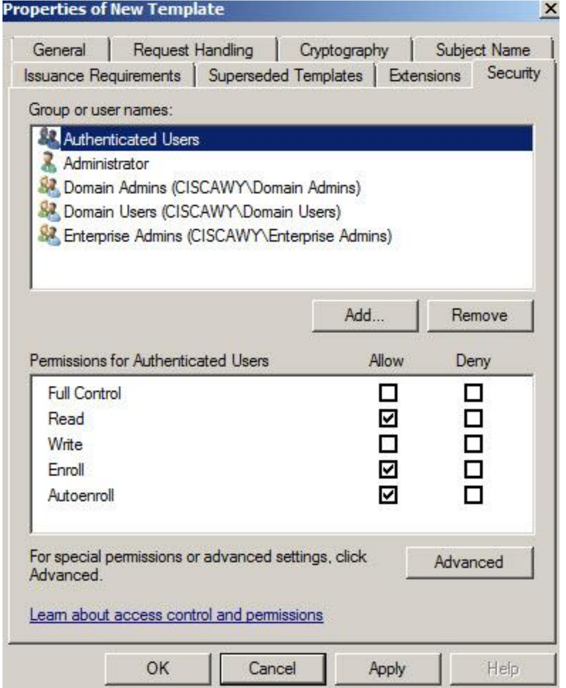
R.click → Cert Template → Manage



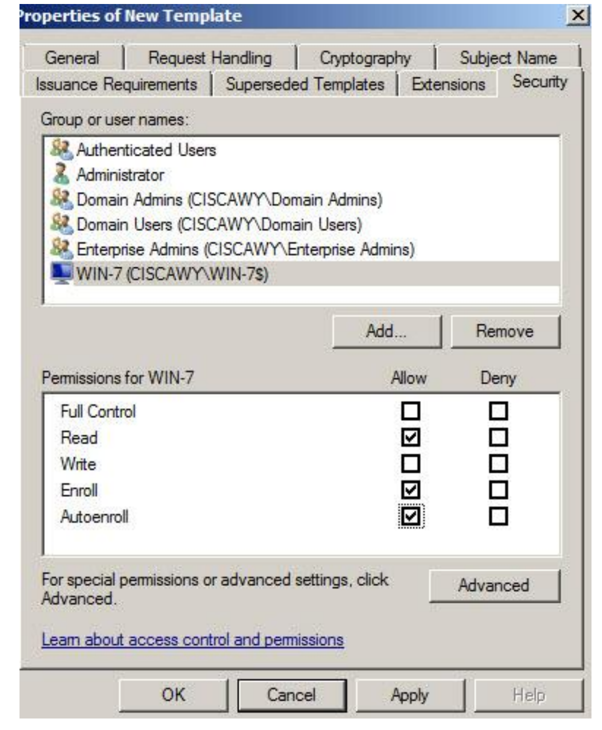
ونختار اي Template ونقوم بعمل Duplicate لها كما فعلنا من سابقا
نقوم بإضافه اسم لها



تختار ال Security
ونضيف لل Authenticated صلاحيات الEnroll و الAutoenroll

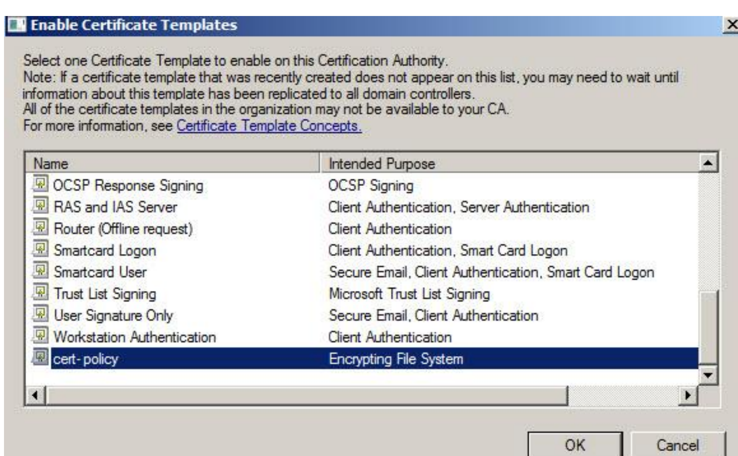


ونقوم أيضا بإضافه الComputer الخاص بWin-7 وزيادة صلاحياته الEnroll و الAutoenroll

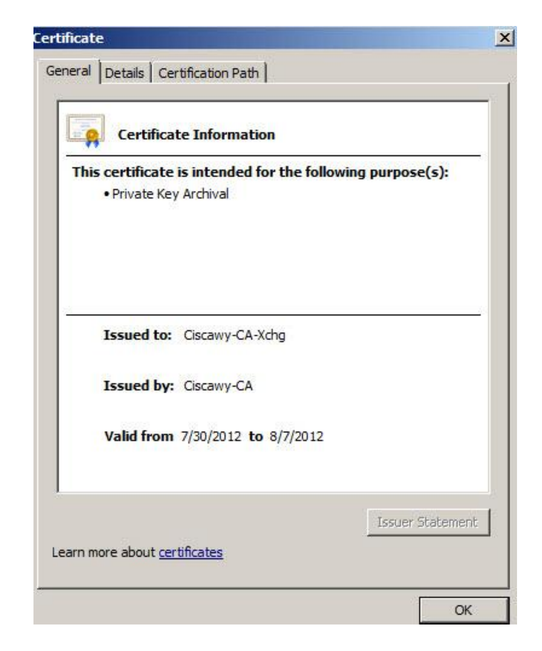


نقوم بعد ذلك بإضافتها

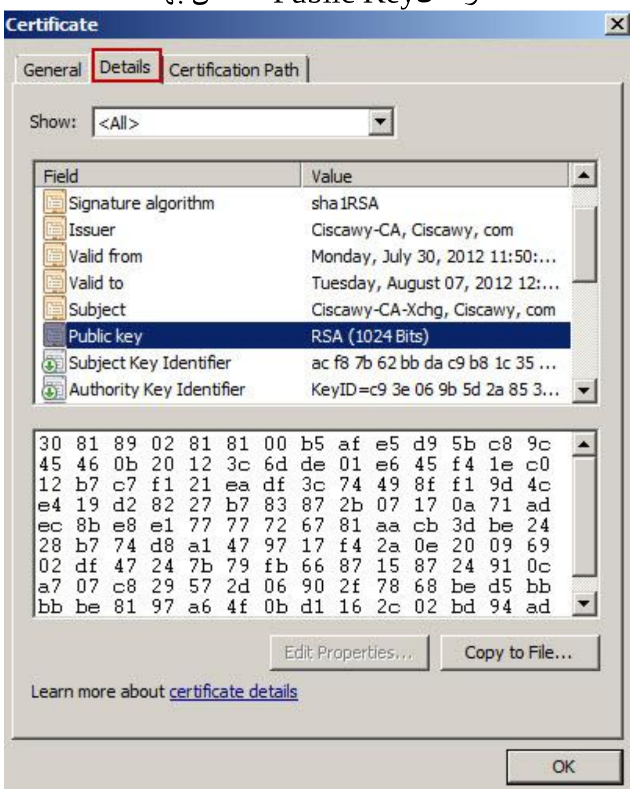




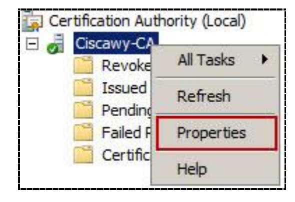
اذا قمنا بعمل D.click علي اي Cert
Issued by اسم الServer اللي عمل ليها نشر



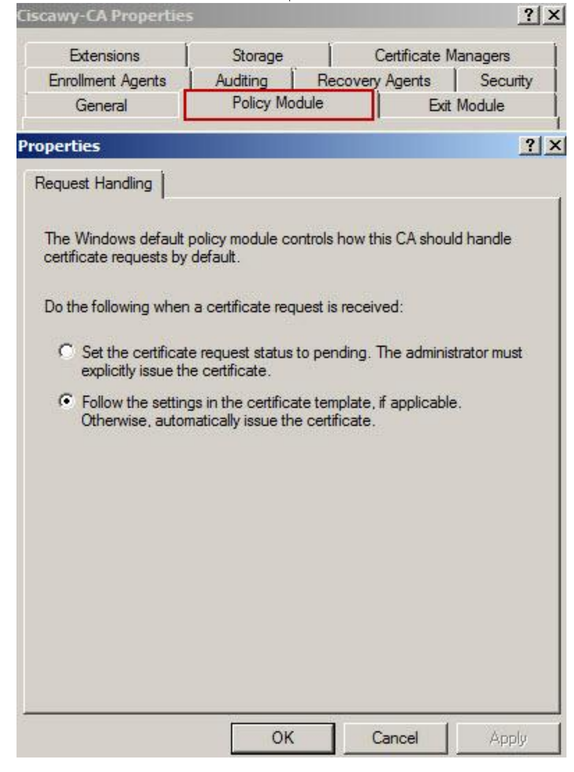
ودا الPublic Key الخاص بها



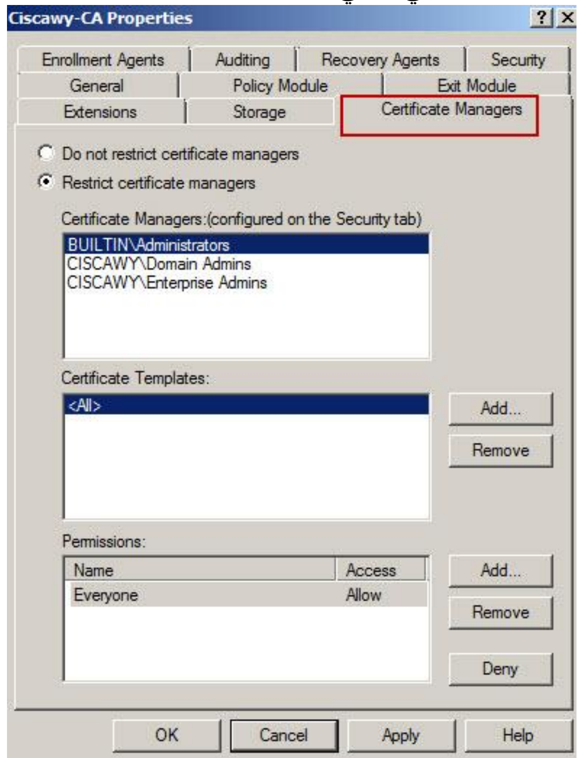
R.click علي اسم ال Domain

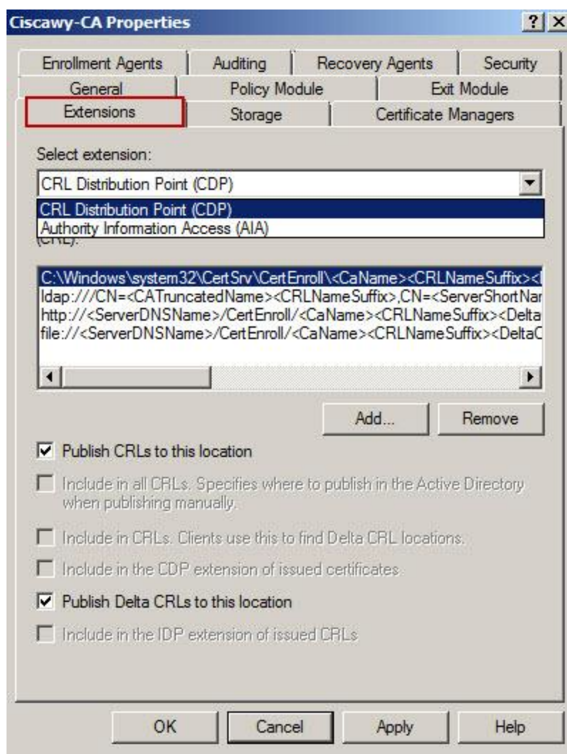


انه يتم نشرها تلقائيا وليس شرطا ان يقوم الAdministrator بعمل Issued لها



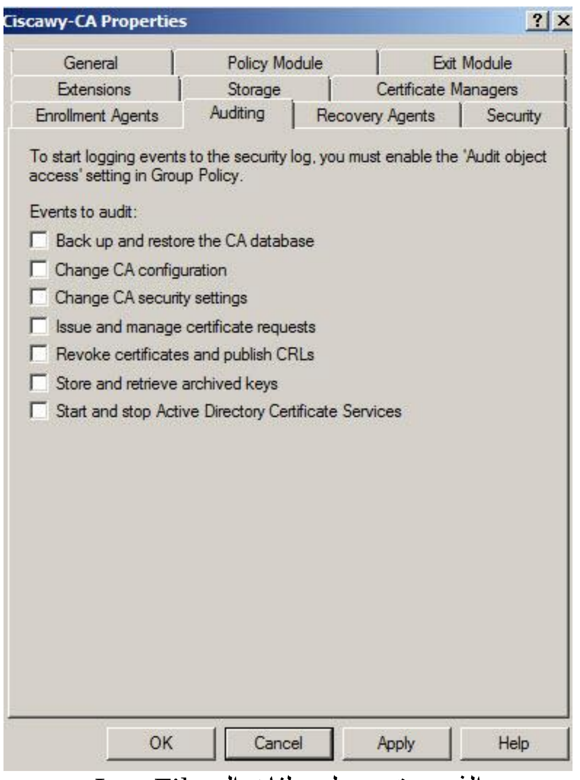
ممكن هنا نضيف الPermissions للمستخدمين ونحددهم
اللي هتبقي الاعدادات الاساسية





CRL → Certificate Revocation List

لو الAdministrator عمل Revoke رفض للSub-ordinate الذي يحتوي علي كل التعديلات و المعلومات عن الCert يتم ارسال Notification لكل المستخدمين انه تم الغاءه



الذي يحتوي علي ملفات الLog Files

KRA → Key Recovery Agent

- يستخدم في حالة :-

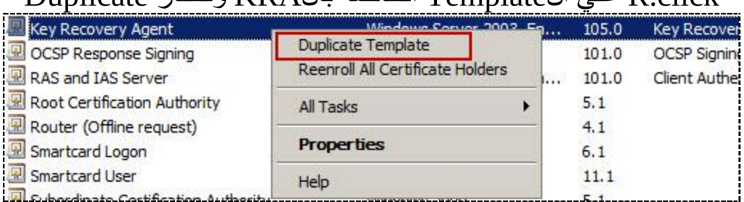
اذا حدث فقد في الCertification الخاصه بمستخدم معين
او حدث فقد في الProfile الخاص به
حيث انه تم استخدامها من قبل الUser في تشفير بعض الملفات او الدخول علي بعض المواقع ومع فقدها لم يعد قادرا علي ان يقوم بفعل شئ او ان يفك تشفير ملفاته

- يجب ان يتم انشاءه قبل ان يقوم أي مستخدم بطلب أي Cert
- مدة صلاحيتها سنتان
- يجب ان نقوم بإنشاء User Account حتي يكون مسئول عن هذه الخدمه ويكون ليه صلاحيات انه يقوم بعمل Recover لأي Cert
- لا بد ان يكون هذا الUser ايضا Member of Domain Admin Group
- نقوم بفتح الCA ونفتح ال Cert Template

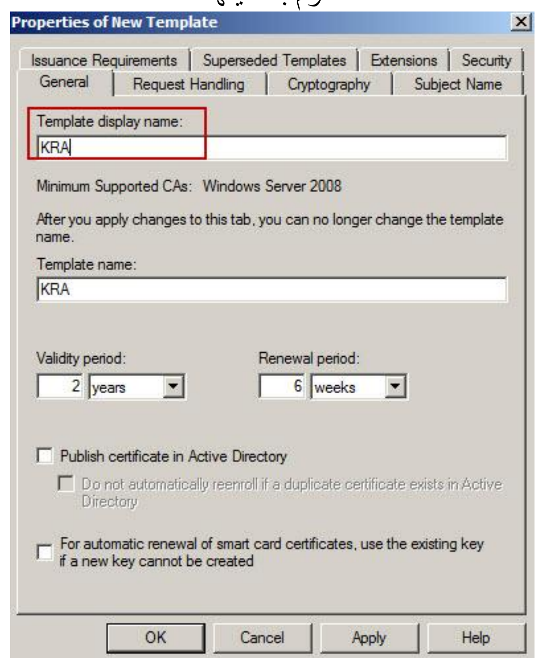
R.click → Manage

Certification Authority (Local)
Ciscawy-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Manage
New
View
Refresh
Export List...
Help

R.click علي الTemplate الخاصه بالKRA ونختار Duplicate

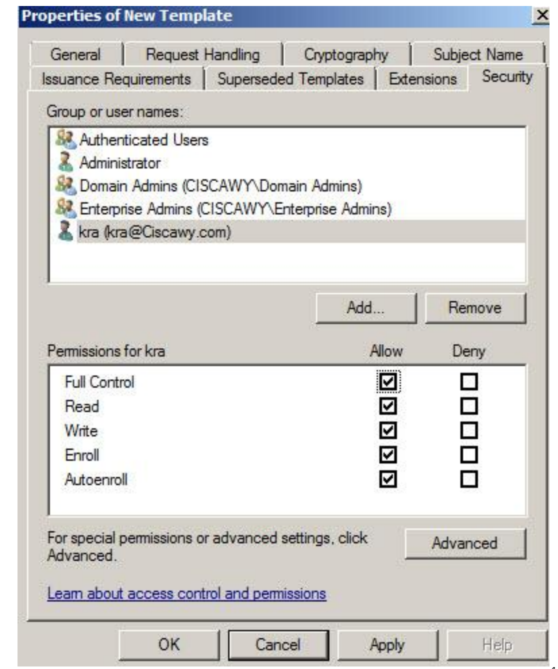


نقوم بتسميتها



نختار الSecurity

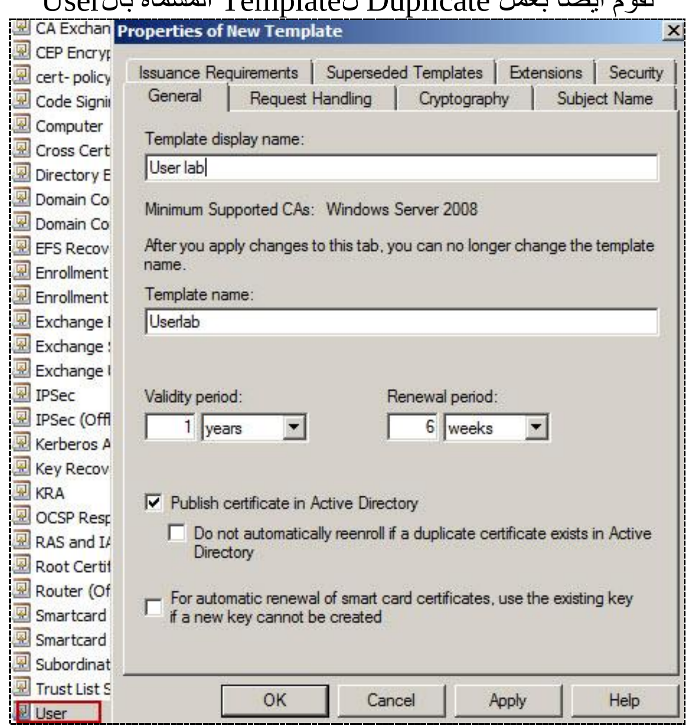
- نضيف الUser الذي تم انشاءه ونضيف له صلاحيات الFull Control



وأيضا نقوم باضافه Full Control لل Authenticated

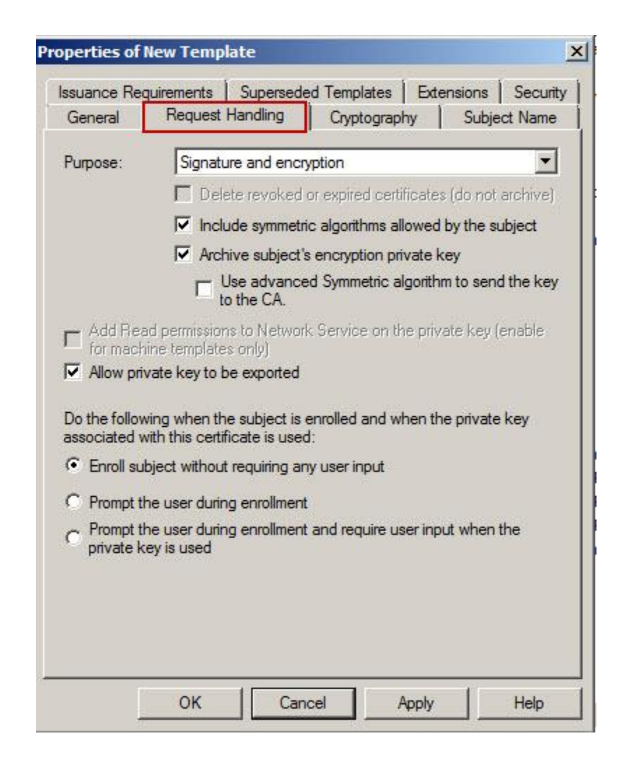
OK → OK

نقوم أيضا بعمل Duplicate لل Template المسماه بالUser



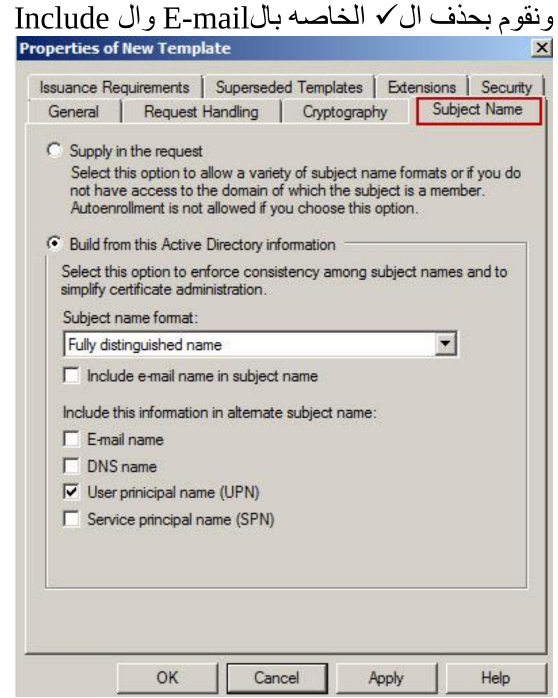
نختار ال Request Handling ونعدلها كما هو موضح

ان ال Private Key الخاص بأي Cert ان يقوم بحفظ ال Private Key الخاص بها

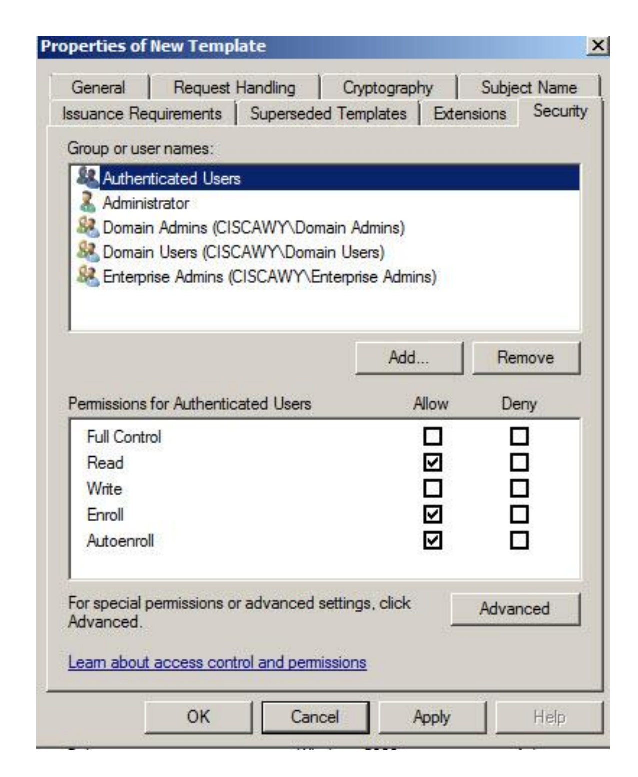


Subject Name

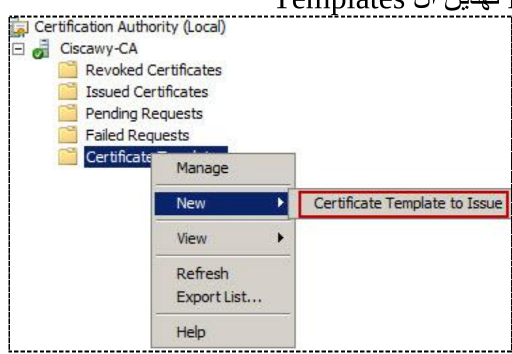
ونقوم بحذف ال✓ الخاصه بالE-mail وال Include



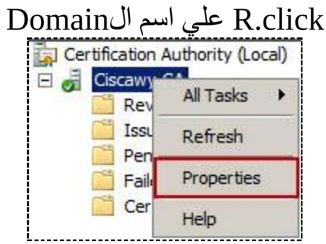
نضيف لل Authenticated صلاحيات Enroll & Autoenroll



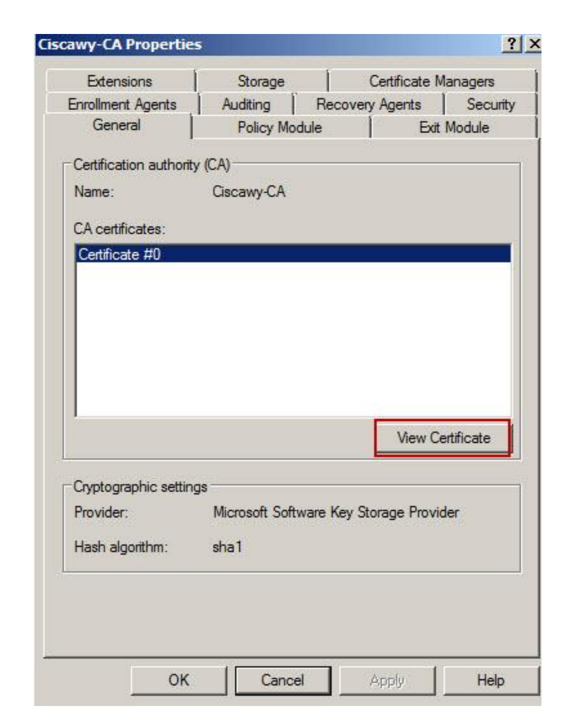
- بعد ذلك نقوم بعمل Issued لهذين ال Templates



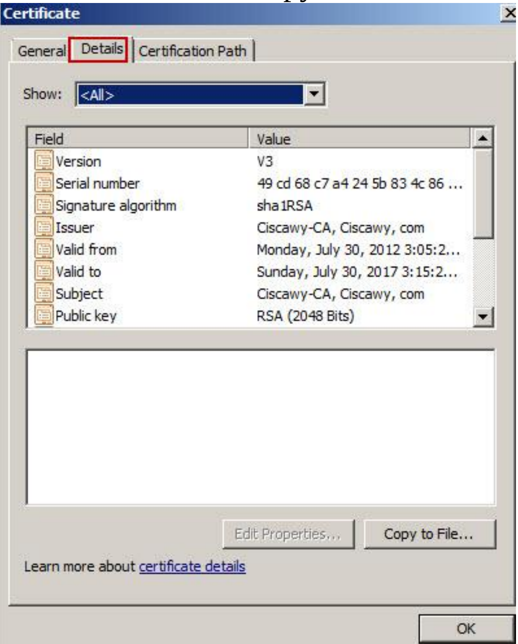
- نقوم بالدخول بحساب الKRA User الذي تم انشاءه في بدايه الفصل
ونقوم بفتح الMMC لعمل Request للCert الخاصه به
نقوم بنسخ الCert الخاصة بالRoot لكي نقوم بتعريف الKRA من هو الRoot
R.click علي اسم الDomain



نختار View Cert



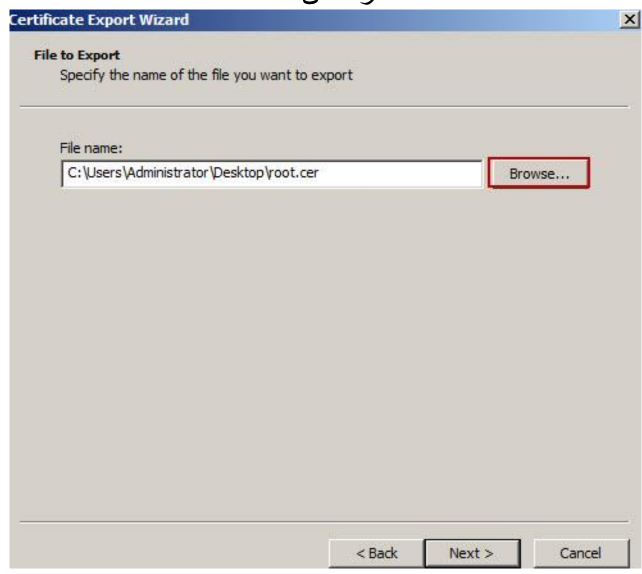
Details → Copy to File





Next → Next

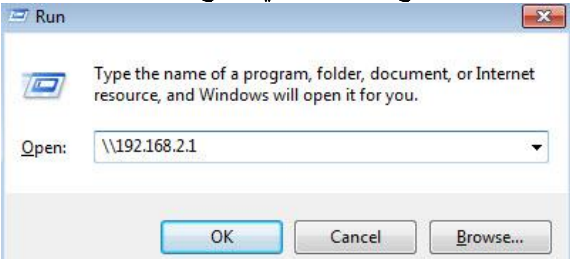
نختار مكان الحفظ





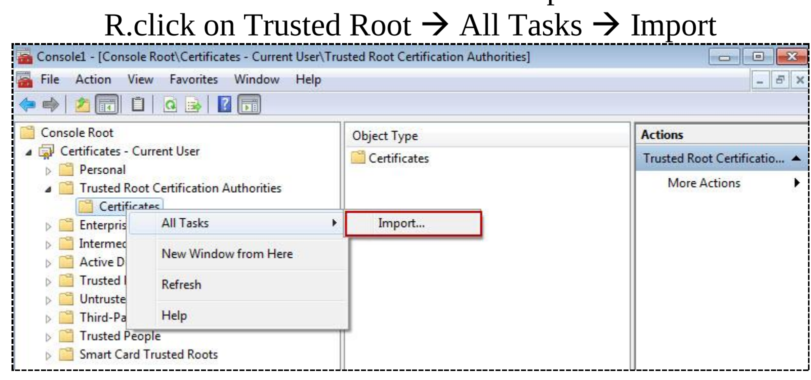
ثم نقوم بوضعها في Shared Folder

- بعد ذلك نقوم بالدخول علي حساب الWin-7
ونقوم بالدخول علي الShared Folder ونسخ الCert علي سطح المكتب



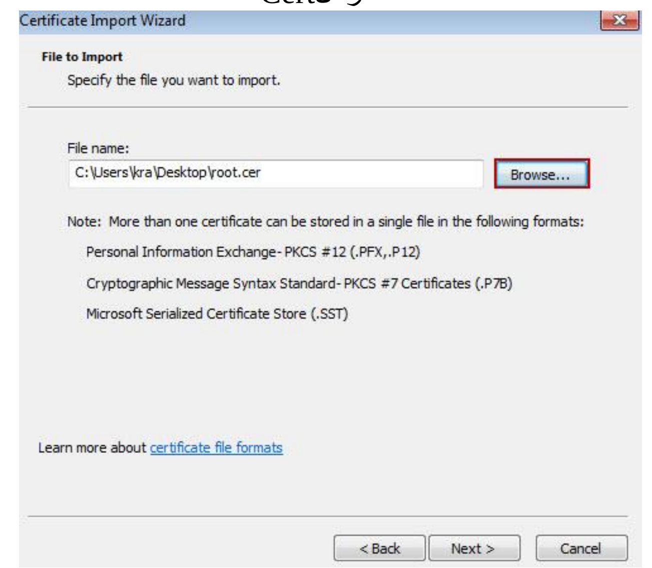
نقوم بفتح Start → Run → MMC

File → Add\Remove Snap-in
R.click on Trusted Root → All Tasks → Import





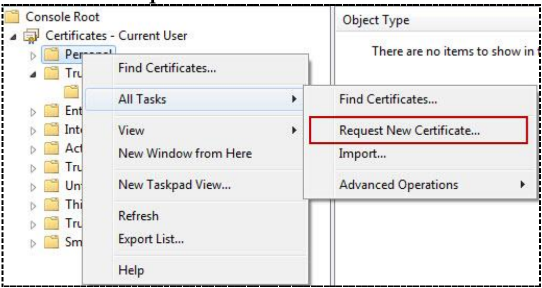
نختار الCert

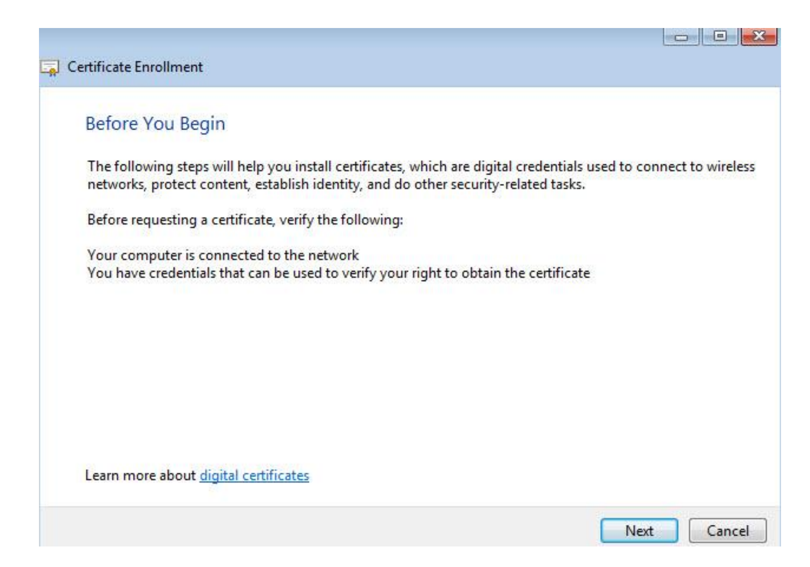


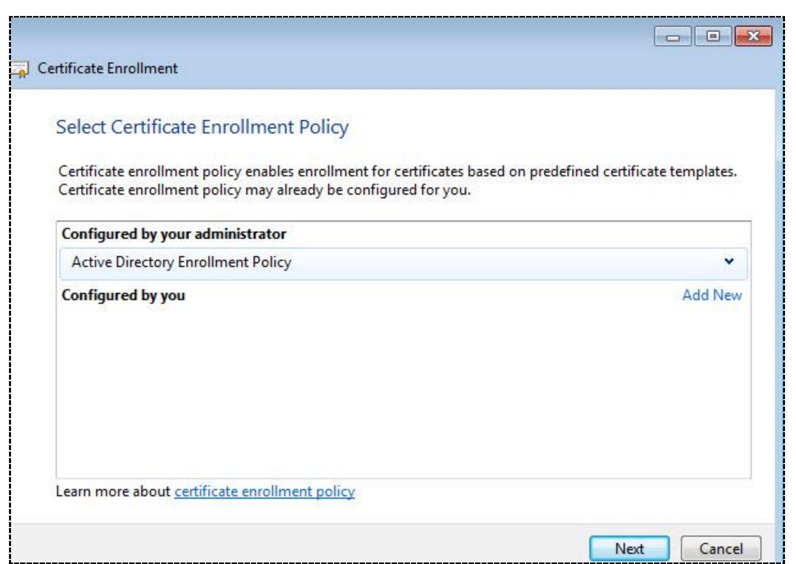
Next → Next



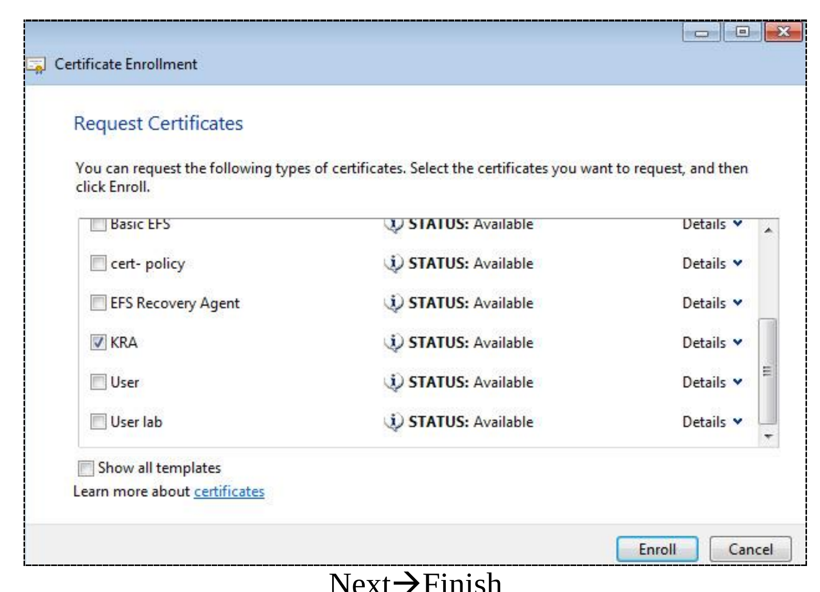
- علي الPersonal نقوم بعمل R.click ونختار Request New Cert







نختار الKRA



Next→Finish

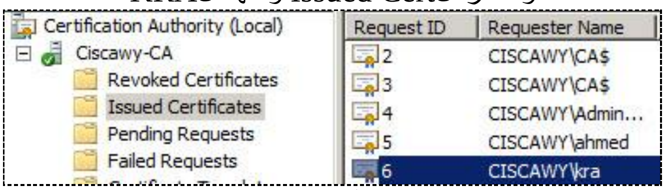
سنلاحظ انه لم يتم اضافتها بعد

حيث ان هذه الCert هي الوحيده التي يجب ان يقوم الAdministrator بعمل Issued من علي ال Root CA لها نظرا لأهميتها

- نقوم بالدخول علي الServer

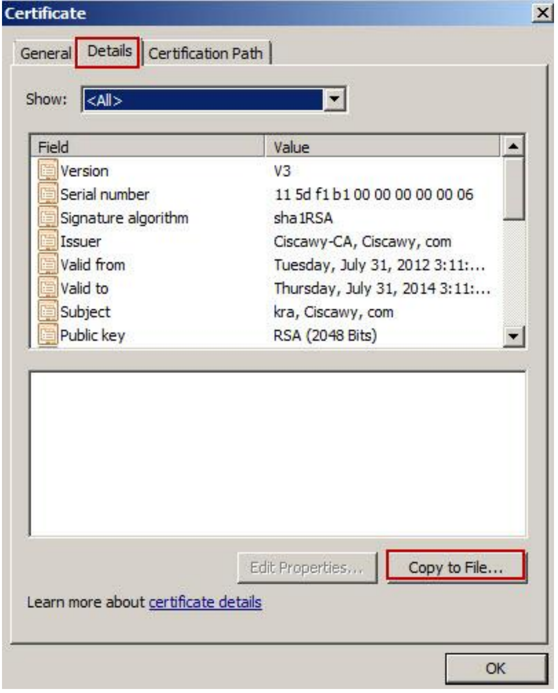
ونقوم بفتح الCA

ونختار الIssued Cert ومنها الKRA



نقوم بالضغط D.Click عليها

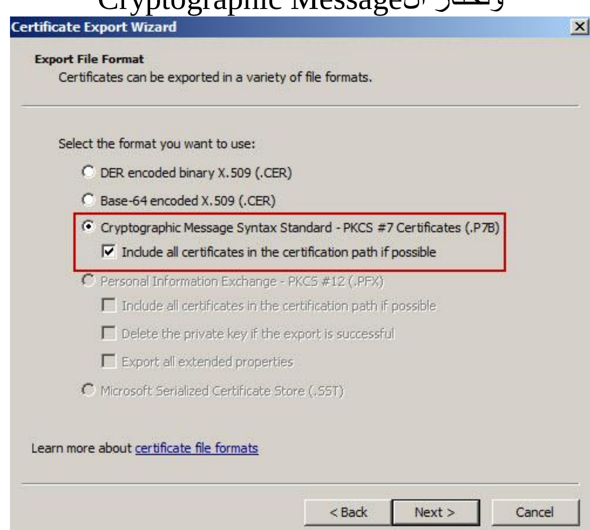
ونختار Details



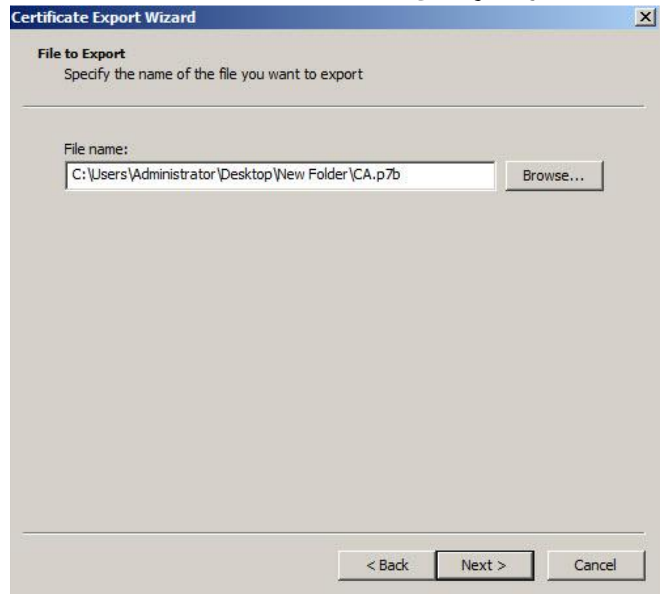
ومنها Copy to File



ونختار الCryptographic Message



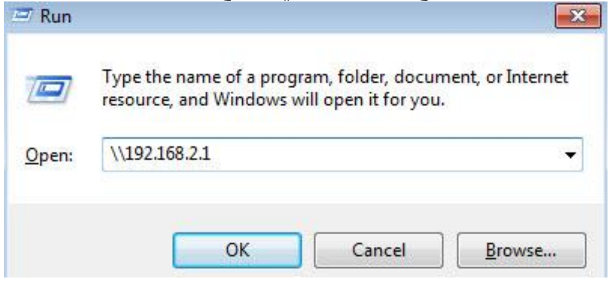
ونختار مكان الحفظ لهذه الـCert





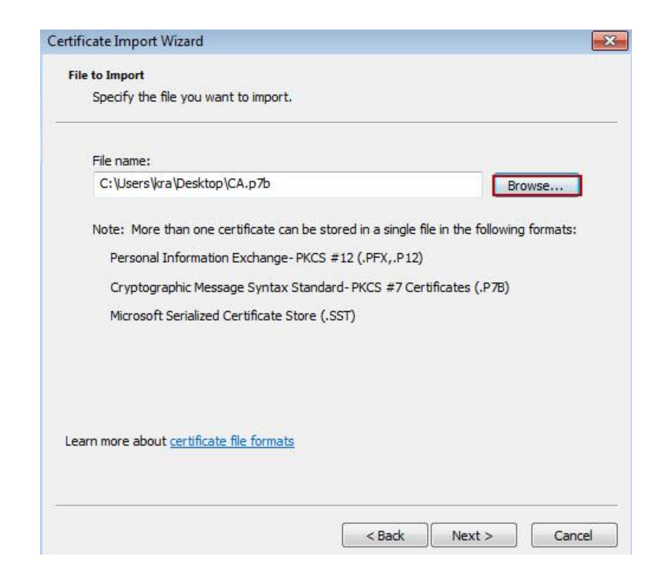
ثم نقوم بوضعها في Shared Folder او نضعها في نفس ال Shared السابق

- بعد ذلك نقوم بالدخول علي حساب الWin-7
ونقوم بالدخول علي الShared Folder ونسخ الCert علي سطح المكتب

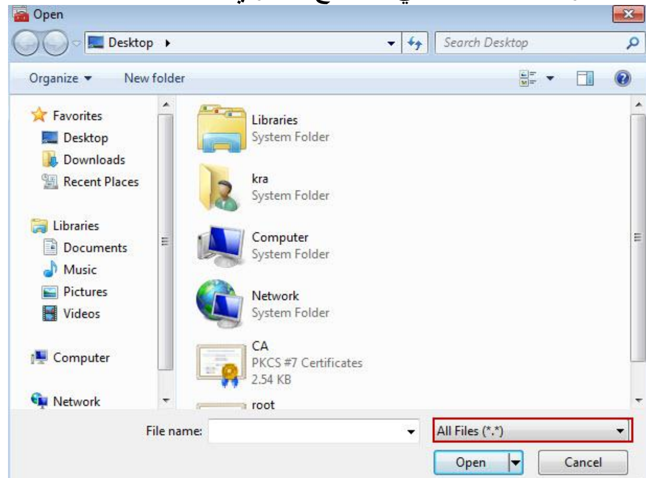


نقوم بفتح MMC → Run → Start
File → Add\Remove Snap-in
R.click on Personal → All Tasks → Import





نختار All Files حتي نستطيع ان نري الامتداد الخاص بها

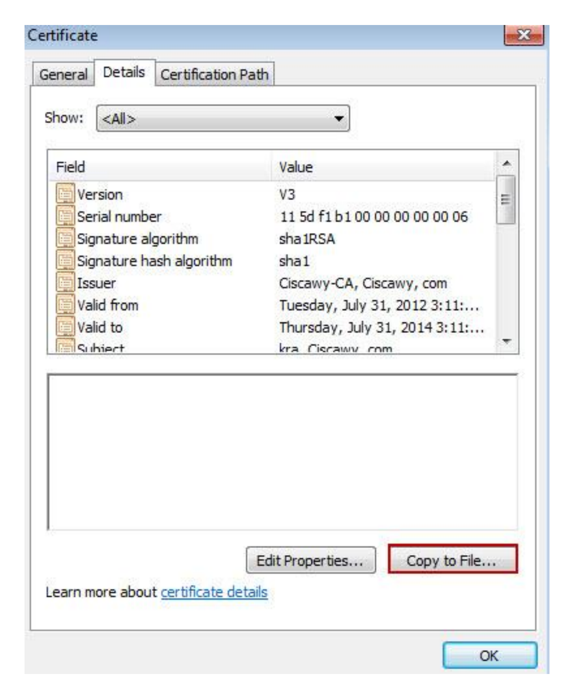


Next → Finish



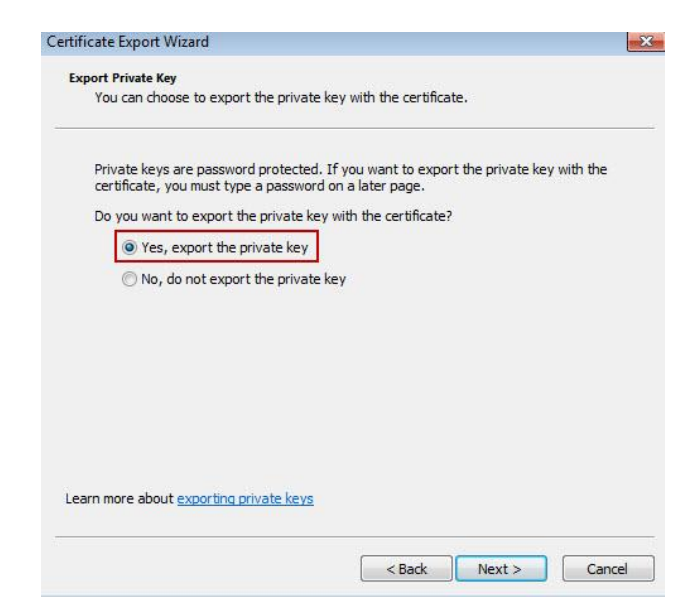
- سنجد انه تم اضافه Two Certifications
احداهما للKRA والاخري خاصه بالRoot

- نقوم بالضغط D.Click علي الCert الخاصه بالKRA
Details → Copy to File

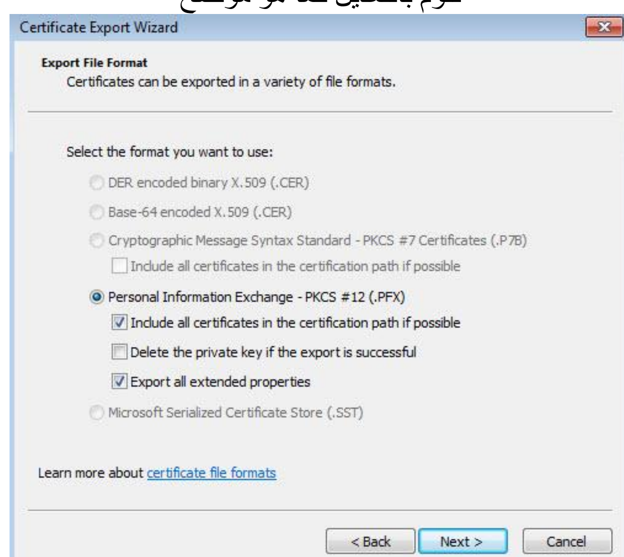




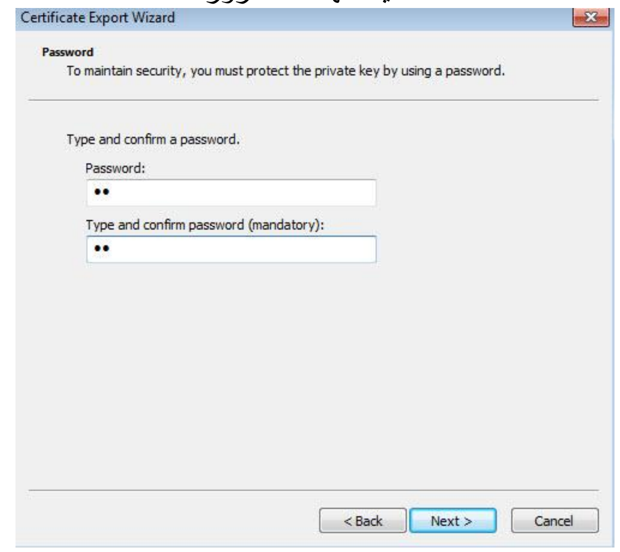
نختار ان يتم اضافه الPrivate Key معها
حيث انه عندما تقوم بعمل Import و Export لأي Cert يحدث تغيير في الKey الخاص بها

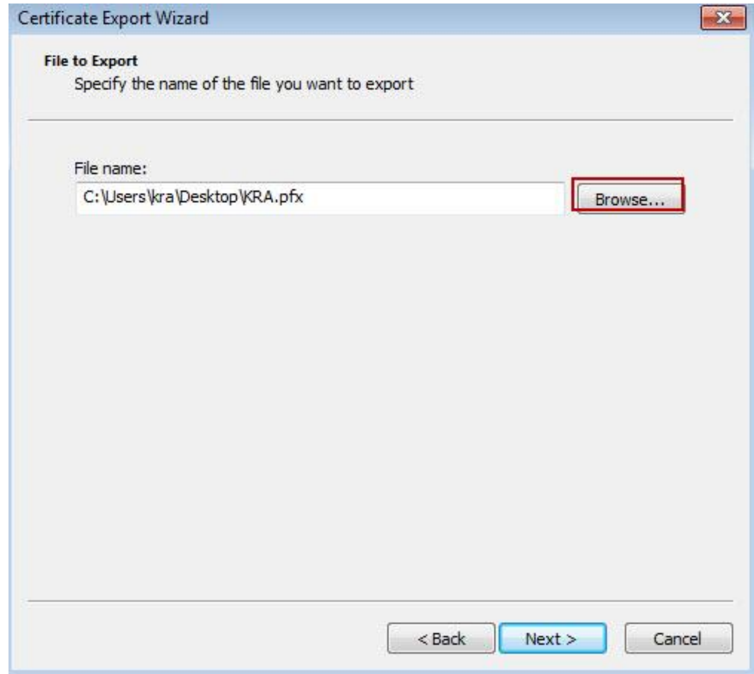


نقوم بالتعديل كما هو موضح



نضيف لها كلمه مرور





نقوم بإختيار مكان للحفظ

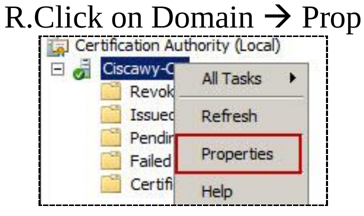
Next → Next



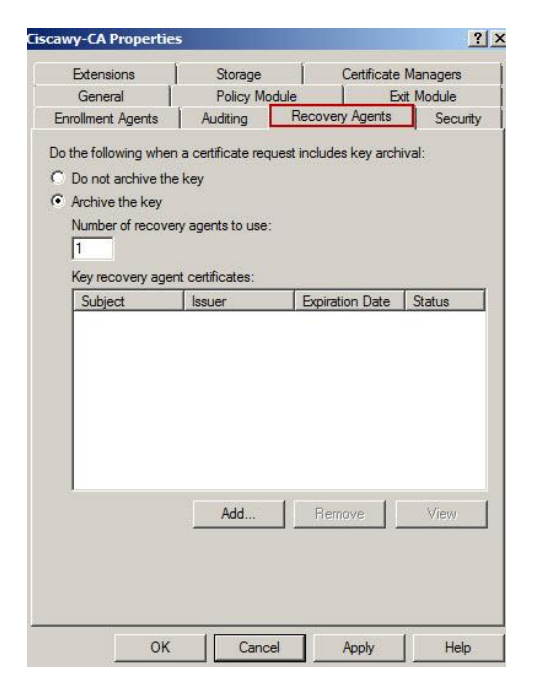
وبعد ذلك نقوم بحفظها في مكان هام جدا حتي لا نفقدها

- نقوم بتعريف الRoot CA ان هناك KRA

R.Click on Domain → Prop

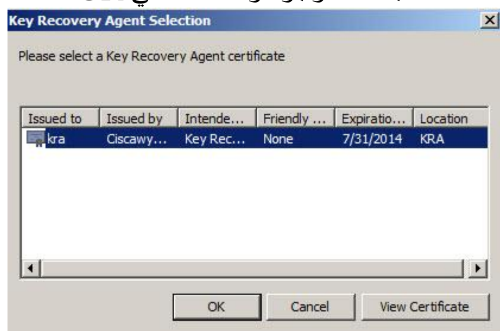


نختار الRecovery Agent ونختار Archive the Key

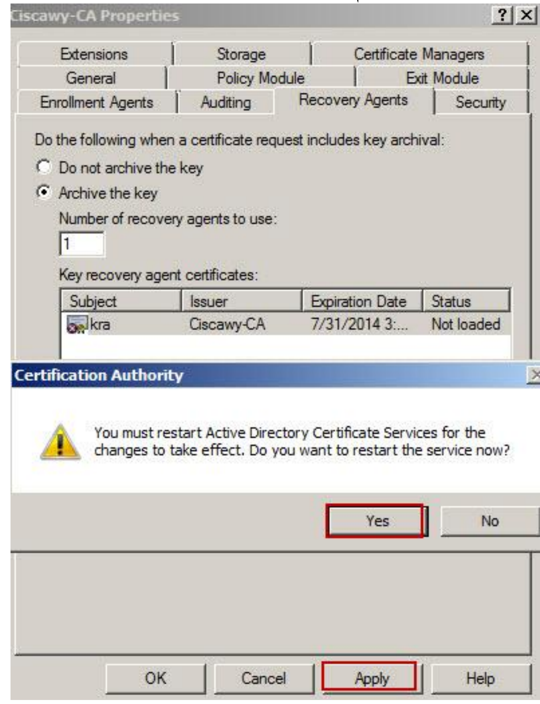


ونقوم بالضغط علي Add

سنجد انه موجود ونضغط علي OK



سيطلب ان يقوم بعمل اعاده تشغيل للService





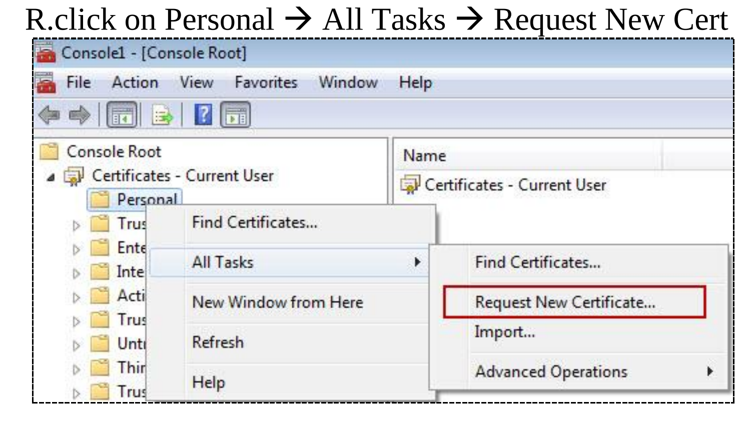
ستجد انها اصبحت Valid واذا حدث اي Error نقوم بإعاده تشغيلها مره اخري

- علي جهاز الWin-7 نقوم بالدخول بأي حساب مستخدم آخر

نقوم بفتح Start → Run → MMC

File → Add\Remove Snap-in

R.click on Personal → All Tasks → Request New Cert



ونختار الCert الخاصه بالUser التي تم نسخها من قبل

Certificate Enrollment

Request Certificates

You can request the following types of certificates. Select the certificates you want to request, and then click Enroll.

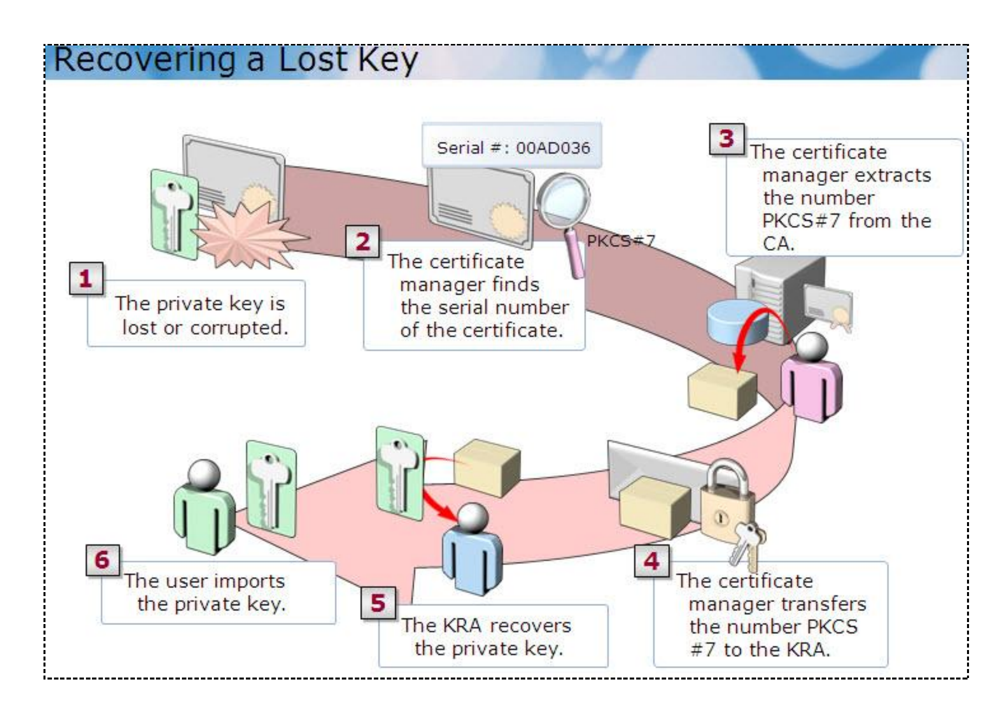
Ahmed-crt	STATUS: Available	Details
Basic	STATUS: Available	Details
Basic EFS	STATUS: Available	Details
cert- policy	STATUS: Available	Details
User	STATUS: Available	Details
☑ User lab	STATUS: Available	Details

Show all templates

Learn more about certificates

Enroll Cancel

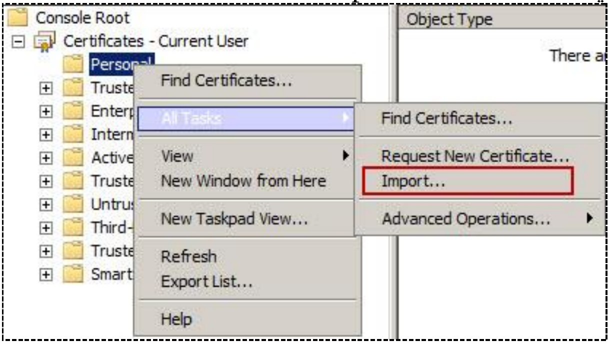
Enroll → Next → Finish



- ولكن ماذا يحدث اذا تم فقد هذه الCert ؟!!!

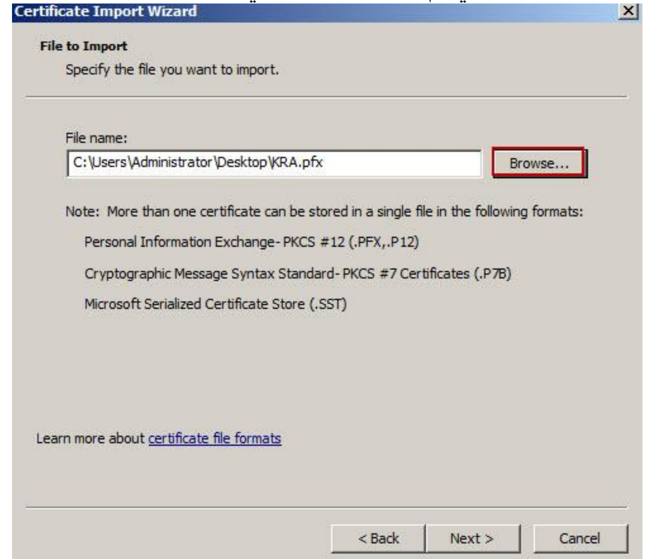
نقوم بالدخول بحساب الKRA علي الMachine الخاصه بالCA
ولكن في هذه الحاله تم انشاء Profile جديد خاص به ويجب علينا ان نقوم بإضافه الCert KRA الخاصه به مره اخري

نقوم بفتح الCA ونضغط علي Personal ومنها Import → All Tasks

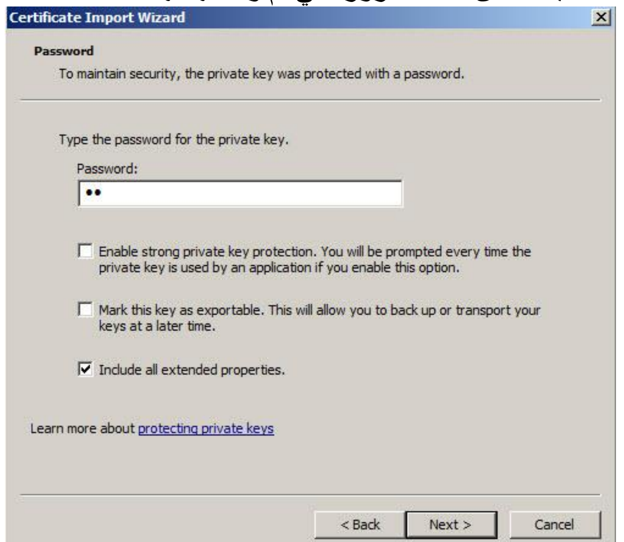




نقوم بإضافه الCert التي تم نسخها من قبل في الاعدادات الاوليه لهذا الفصل

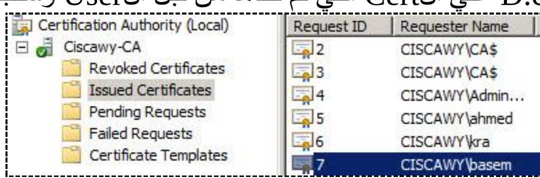


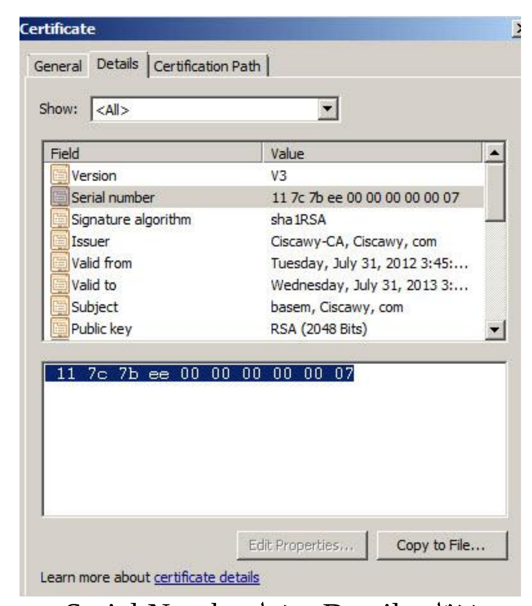
يسأل عن كلمه المرور التي تم وضعها لهذه الCert





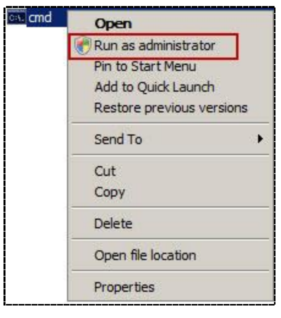
نقوم بالضغط D.click علي الCert التي تم فقدها من قبل الUser وسنجدها في الIssued





نختار Details ومنها Serial Number
ونقوم بنسخه Ctrl+C حتي نستخدمه في عمليه الRecovery
لأننا حينما قمنا بعمل Import لهذه الCert قمنا بنسخ الPrivate Key الخاص بها

- نقوم بفتح الRun ونضغط عليها R.Click → Run as Administrator



نقوم بكتابه
Certutil –getkey " Serial Numer For Cert that Copied" file name
Certutil –getkey
بعد ذلك في " " يتم وضع الرقم الخاص بهذه الCert
ويتم وضع اسم لهذه ال Cert

```
C:\Windows>certutil -getkey "11 7c 7b ee 00 00 00 00 00 07" basem
Querying CA.Ciscawy.com\Ciscawy CA......................

"CA.Ciscawy.com\Ciscawy-CA"
  Serial Number: 117c7bee000000000007
  Subject: CN=basem, DC=Ciscawy, DC=com
  UPN:basem@Ciscawy.com
  NotBefore: 7/31/2012 3:45 PM
  NotAfter: 7/31/2013 3:45 PM
  Template: Userlab, User lab
  Version: 3
  Cert Hash(sha1): 45 9a 4c 80 06 91 b6 5d 92 62 66 b9 6c 76 f0 1d 64 50 0f bd

Recipient Info[0]:
CMSG_KEY_TRANS_RECIPIENT(1)
CERT_ID_ISSUER_SERIAL_NUMBER(1)
    Serial Number: 115df1b1000000000006
    Issuer: CN=Ciscawy-CA, DC=Ciscawy, DC=com
    Subject: CN=kra, DC=Ciscawy, DC=com
CertUtil: -GetKey command completed successfully.
```

ثم نقوم بكتابه هذا الامر

```
C:\Windows>certutil -recoverkey basem basem.pfx
```

Certutil –recoverkey
نضيف الاسم السابق
بعد ذلك نضيف الاسم.pfx الامتداد الخاص بالCert

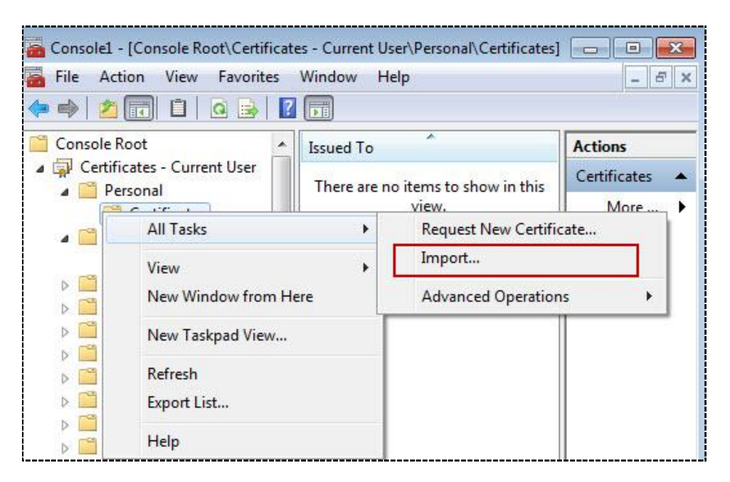
سيطلب ان نقوم بإعطاءه كلمه مرور جديده

```
Enter new password:
Confirm new password:
CertUtil: -RecoverKey command completed successfully.
```

سيتم حفظها علي ال:C\
نقوم بوضعها في Shared Folder

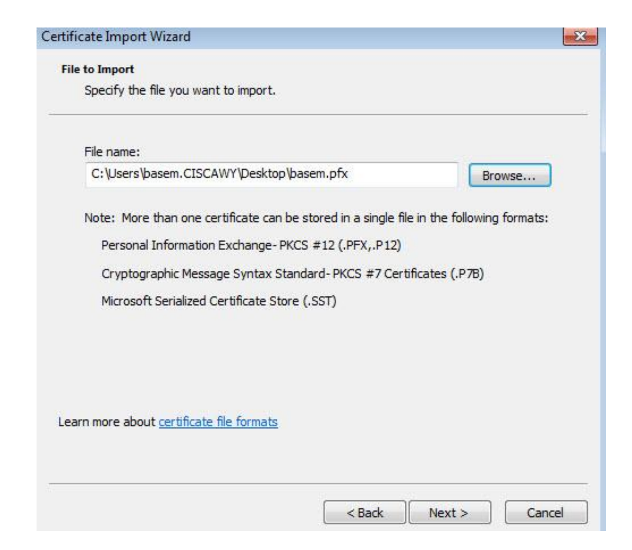
- بعد الانتهاء من هذه الخطوات

نقوم بالدخول علي حساب الWin-7 بصلاحيات ال User الذي فقد الCert الخاصه به
نقوم بفتح مسار الShared Folder ونقوم بنسخ الCert علي سطح المكتب
Start → Run → MMC نقوم بفتح
File → Add\Remove Snap-in
R.click on Personal → All Tasks → Import



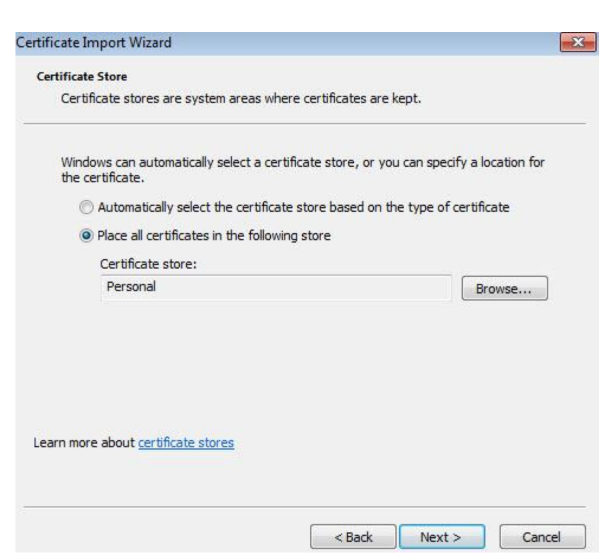


نقوم بإختيار المكان المحفوظه به



نقوم بوضع كلمه المرور الجديده





Next → Next → Finish

سنجد انه تم اضافتها لنجاح للمستخدم ويمكنه استخدامها كما كان يفعل من قبل
وسنلاحظ انه نفس الSN الخاص بها

وبذلك نكون قد انتهينا من عمليه الRecovery بنجاح

Active Directory Rights Management Services

- احدي الخدمات التي كانت موجوده في Windows Server 2003 R2
- تستخدم لتطبيق صلاحيات علي الShared Folder علي الUsers
- ان أي مستخدم ممكن يعمل Access بناء علي NTFS Permissions

- نجري قيود علي الUser انه يتعامل مع الملفات سواء انه ياخد Copy او انه يعمل Print Screen للملف
- بتحدد ايه الصلاحيات اللي ممكن الUser يقوم بها علي هذا الملف
- يشترط ان يكوم المستخدمين نظام التشغيل لهم Win-7 . Vista. XP Sp3
- لو XP SP2 يتم تنزيل Rights Management Client

- الUser الذي سيتعامل مع هذه الخدمة لابد من ان يتم اضافه E-mail في الAttributes الخاصه به والتعديل في خصائص كلمه المرور الخاصه به no password change or expiration

AD RMS Requirements :-

- CAعليه خدمه الDC ان يكون هناك
- يمكن ان نستخدم قاعده البيانات SQL 2005 / 2008 لعمل Hosting
- Officeالتي سيتم عليها اضافه الصلاحيات ونستخدم في الغالب الRMS aware application

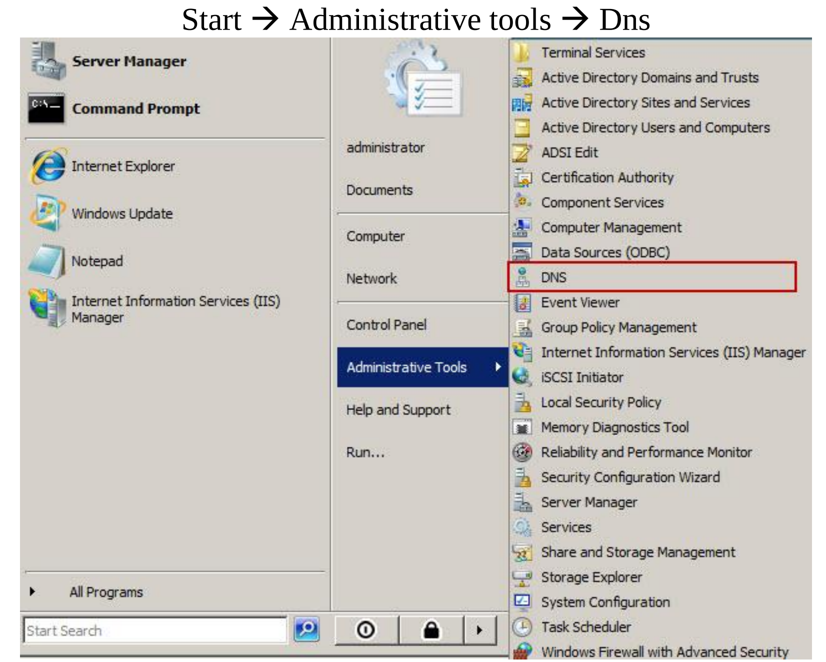
ذا كنا سنستخدمها عليMachine منفصله :-

يتم اضافه CNAME في ال DNS الخاص بال Domain Controller

والCNAMEيقوم بعمليه تحويل من اسم لإسم

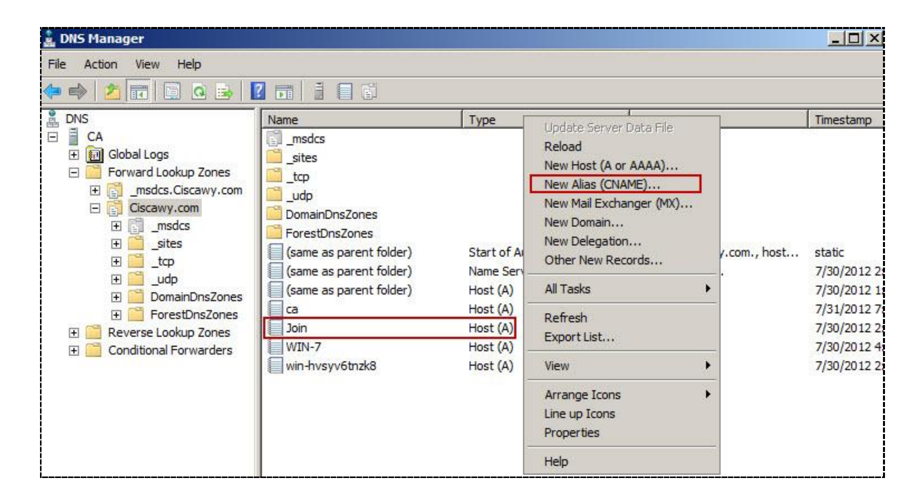
(سنتعرف عليها بالتفصيل في كورس الانفرا)

Start → Administrative tools → Dns

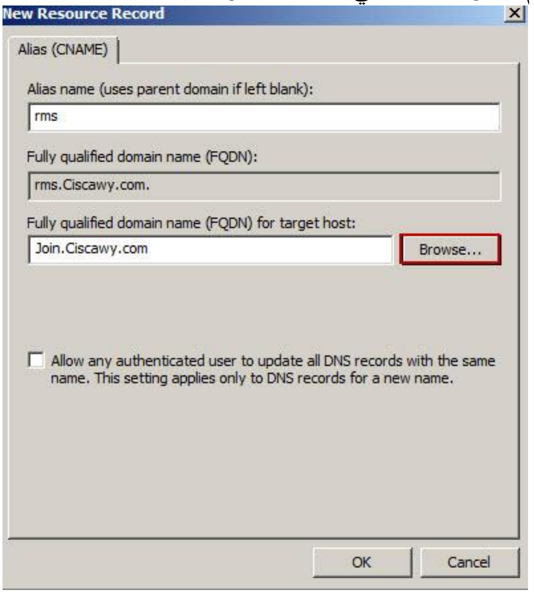


سنلاحظ ان اي Machine مرتبطه بالDomain تم انشاء لها A Record

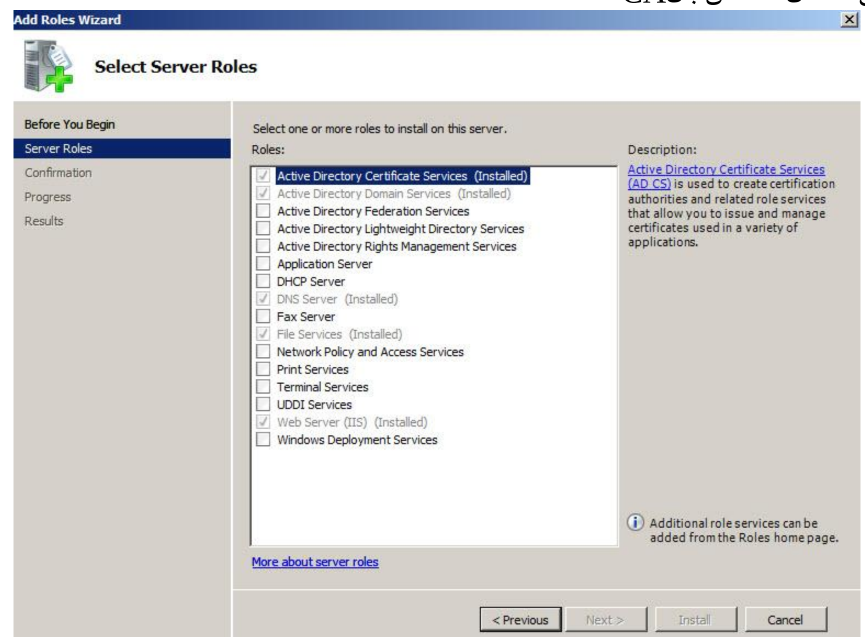
R.click → New CNAME



نضيف اسم ليه ونضغط علي Browse ونضيف الA Record الخاص به



بعد ذلك علي الDomain Controller نقوم بتنزيل خدمتي الCertification Service والIIS وقمت بنصيبهما في الفصل الخاص بالCA



نقوم بفتح الCA لتعديل في الTemplate الخاصه بالWeb Server

Server Manager → AD SC → Cert Template

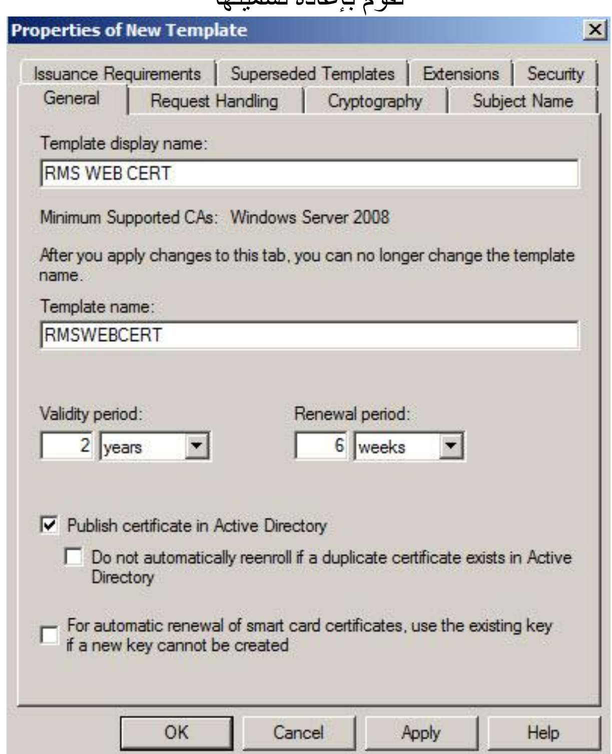
Server Manager (CA)
- Roles
  - Active Directory Certificate Services
    - Enterprise PKI
    - Certificate Templates (CA.Ciscawy.com)
    - Ciscawy-CA
  - Active Directory Domain Services
  - DNS Server
  - File Services
  - Web Server (IIS)
- Features
- Diagnostics
- Configuration
- Storage

Certificate Templates (CA.Ciscawy.com)

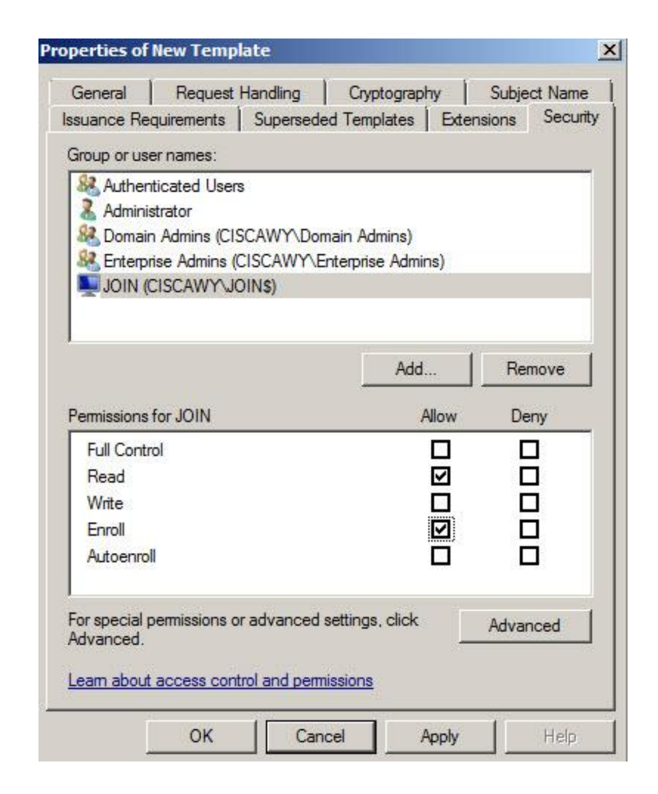
Template Display Name	Minimum Supported CAs	Version
Code Signing	Windows 2000	3.1
Computer	Windows 2000	5.1
Cross Certification Authority	Windows Server 2003, En...	105.0
Directory Email Replication	Windows Server 2003, En...	115.0
Domain Controller	Windows 2000	4.1
Domain Controller Authentication	Windows Server 2003, En...	110.0
EFS Recovery Agent	Windows 2000	6.1
Enrollment Agent	Windows 2000	4.1
Enrollment Agent (Computer)	Windows 2000	5.1
Exchange Enrollment Agent (Offline request)	Windows 2000	4.1
Exchange Signature Only	Windows 2000	6.1
Exchange User	Windows 2000	7.1
IPSec	Windows 2000	8.1
IPSec (Offline request)	Windows 2000	7.1
Kerberos Authentication	Windows Server 2003, En...	110.0
Key Recovery Agent	Windows Server 2003, En...	105.0
KRA	Windows Server 2008	100.1
OCSP Response Signing	Windows Server 2008	101.0
RAS and IAS Server	Windows Server 2003, En...	101.0
Root Certification Authority	Windows 2000	5.1
Router (Offline request)	Windows 2000	4.1
Smartcard Logon	Windows 2000	6.1
Smartca	Windows 2000	11.1
Subordi	Windows 2000	5.1
Trust Li	Windows 2000	3.1
User	Windows 2000	3.1
User lab	Windows Server 2008	100.2
User Sig	Windows 2000	4.1
Web Server	Windows 2000	4.1
Workstation Authentication	Windows Server 2003, En...	101.0

Duplicate Template
All Tasks
Properties
Help

نقوم بإعاده تسميتها



نختار الSecurity ونضيف الComputer Account الذي سنقوم بتنزيل عليه خدمه الRMS
واضافه ✓ علي Enroll

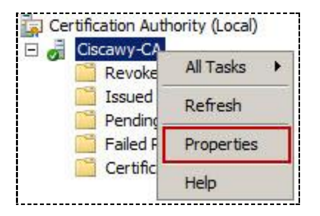


ثم بعد ذلك نقوم بعمل Issue لها (كما عرفنا من قبل)

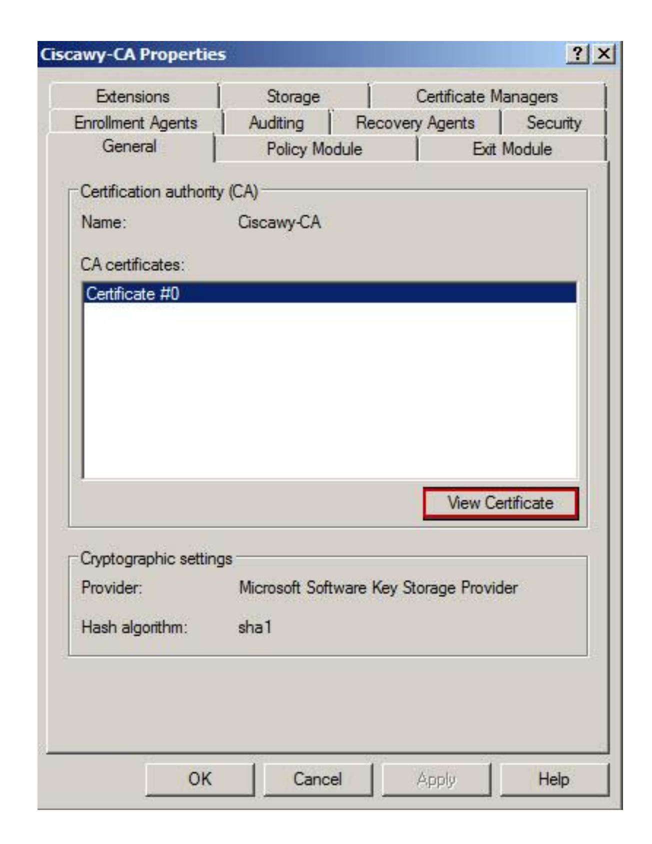


الان نقوم بعمل Export للCert

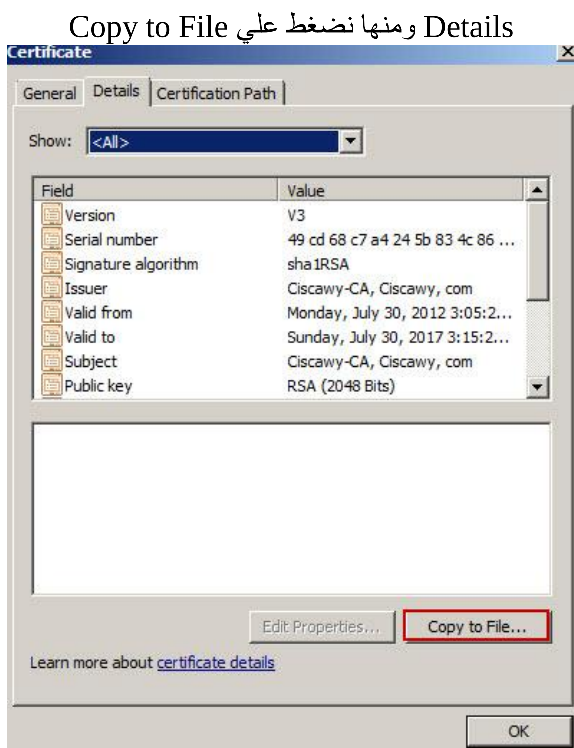
R.click on Ciscawy-CA → Properties



نختار View Cert

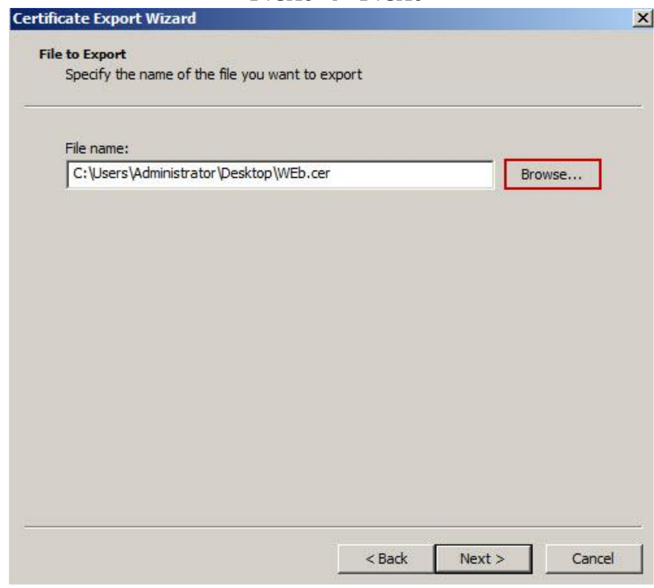


Copy to File ومنها نضغط علي Details





Next → Next



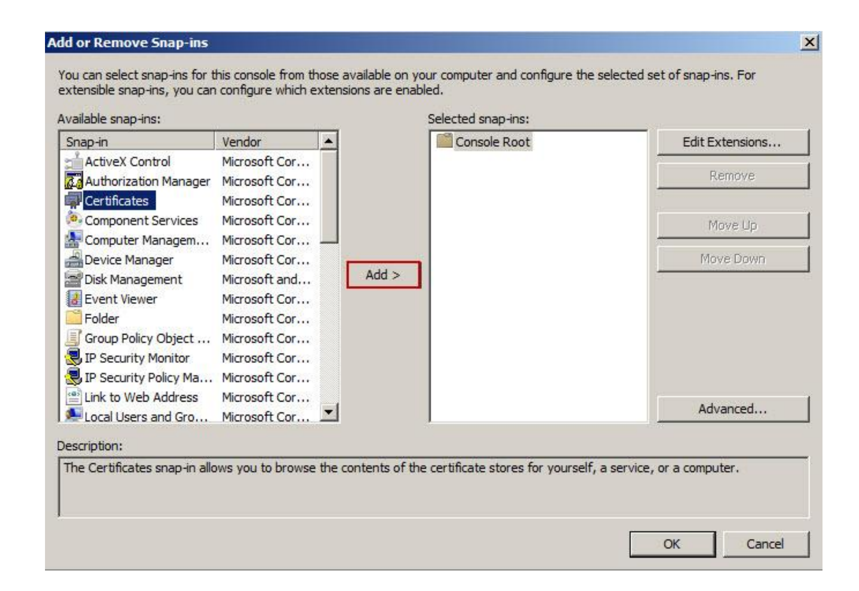
ونختار مكان الحفظ

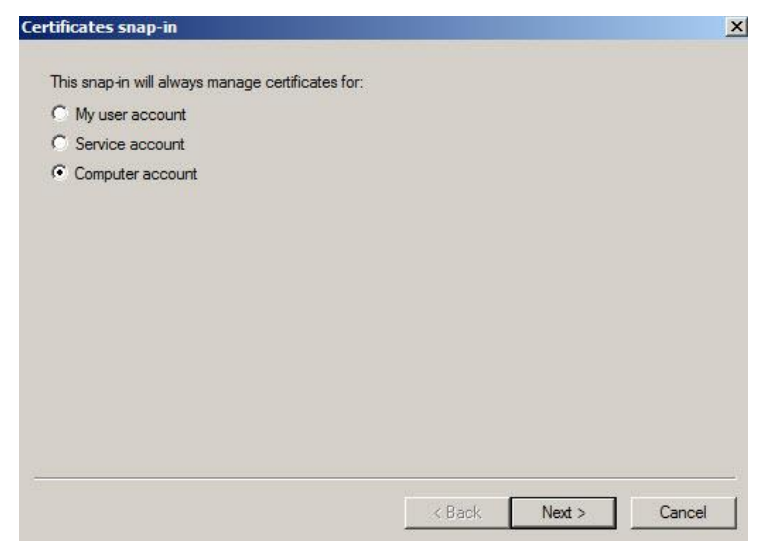


بعد ذلك نقوم بوضعها في Shared Folder

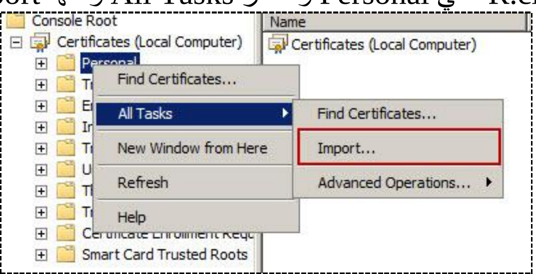
علي الMachine الأخري نقوم بفتح المسار الخاص بالShared Folder
ونسخ الCert علي سطح المكتب

نقوم بفتح الMMC ← run ← Start
File → Add\Remove Snap-in
Cert → Add






R.click علي Personal ونختار All Tasks ومنها Import





Next → Next

نختارها من علي سطح المكتب



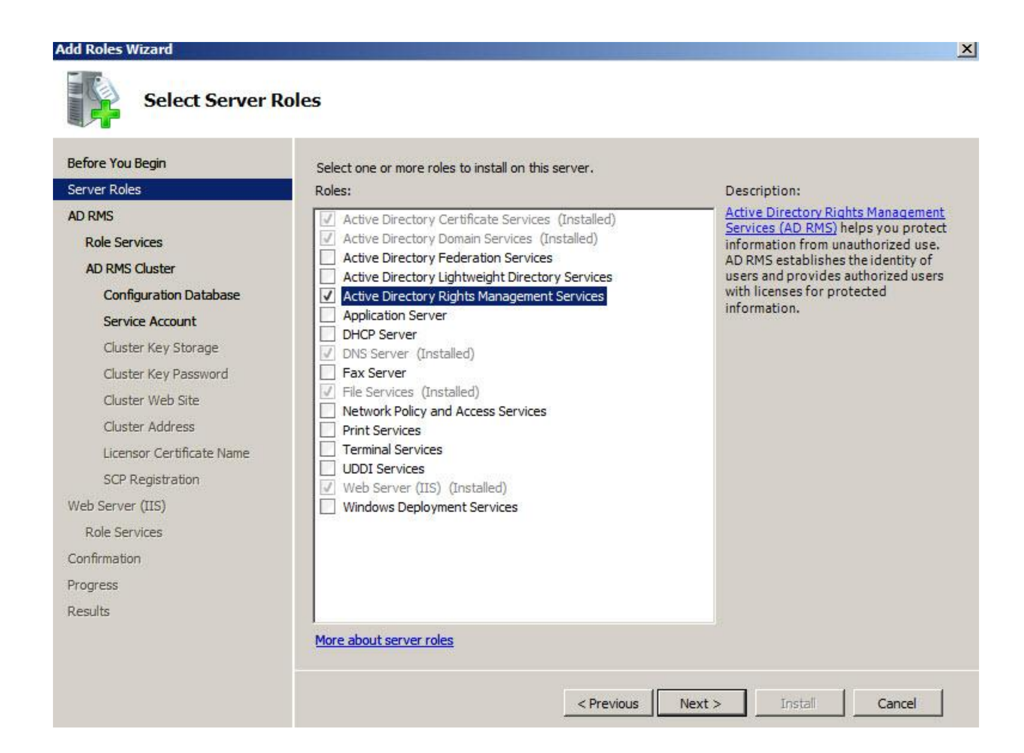
Next



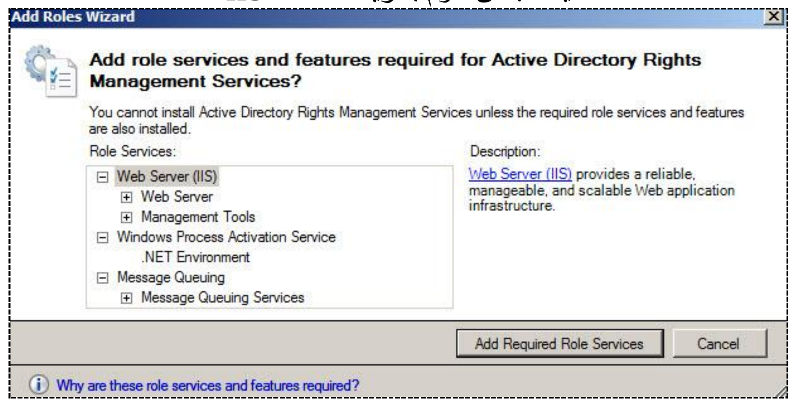
بعد ذلك نقوم بعمل Request New Cert واضافتها

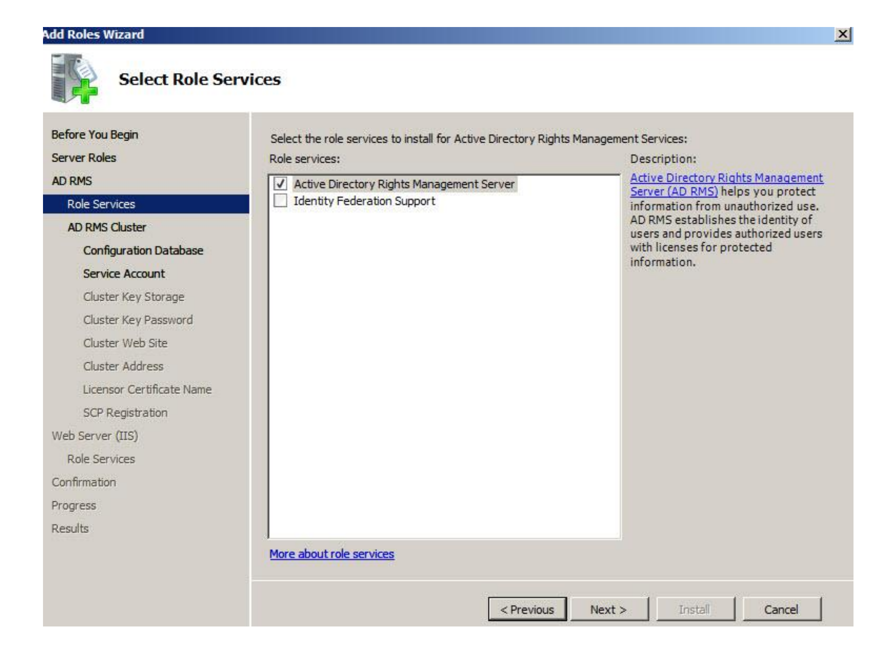
◊ ولكن حاليا بما ان في بيئه Lab سنقوم باستخدامها علي نفس الMachine التي تلعب دور ال Domain Controller

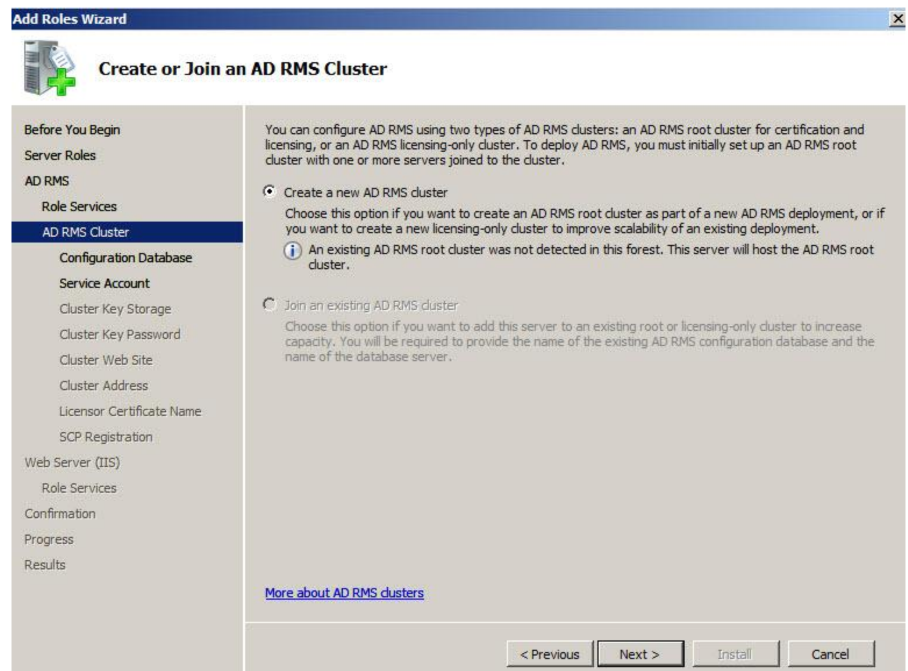
نقوم بفتح Server Manager → Roles → Add Role
نختار AD RMS



يتطلب ان نقوم بتنزيل خدمه الIIS

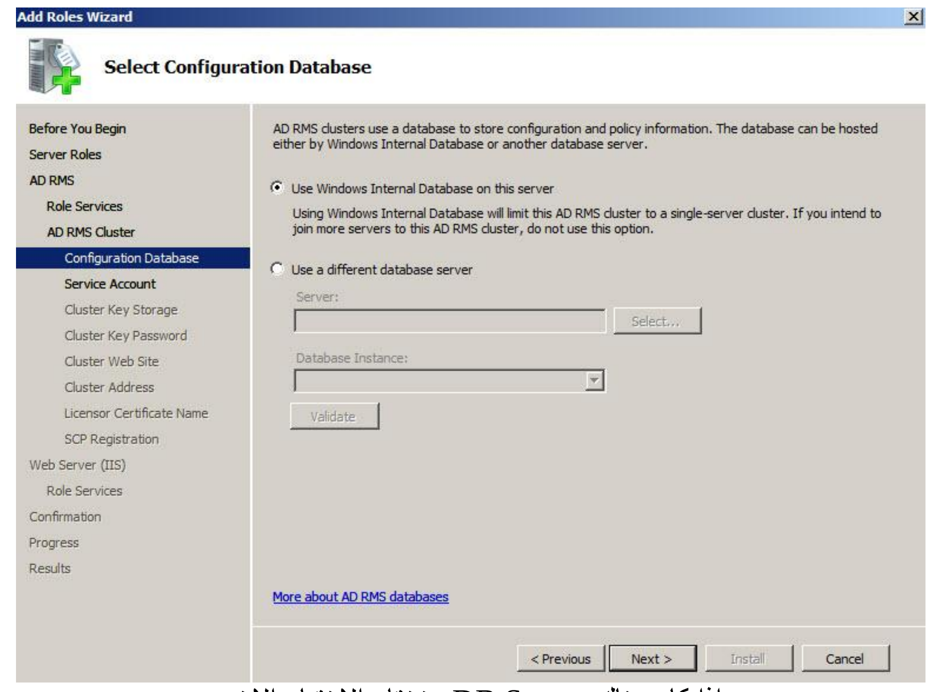




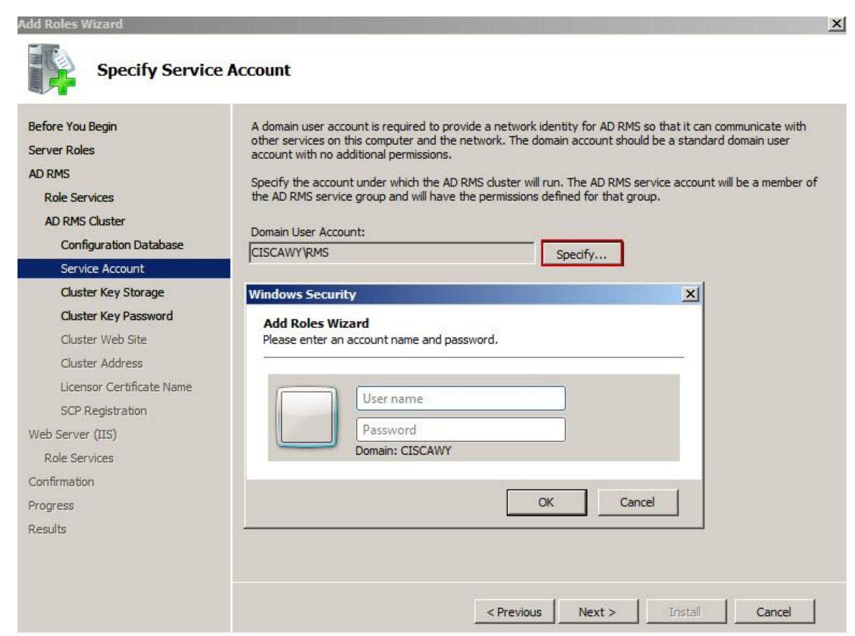


نقوم بإنشاء نفس الCluster

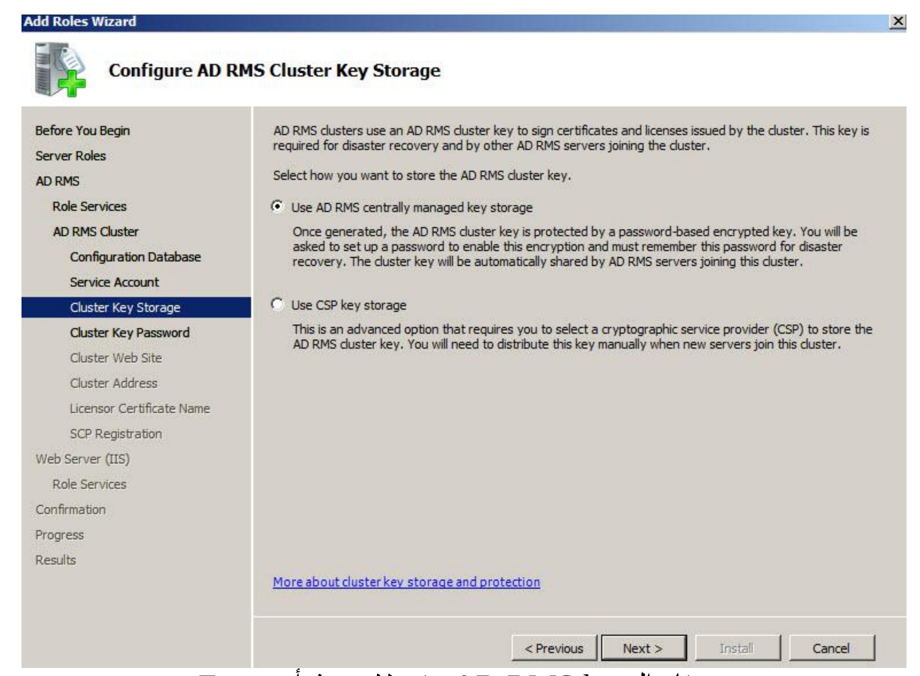
الCluster مجموعه من الاجهزه مشتركه مع بعضها وتقدم خدمه موحده و هذا لعمل ما يسمي بال Load Balancing
وحيث ان هذا هو اول Server يقدم هذه الخدمه سنقوم بإنشاء Cluster جديد عليه



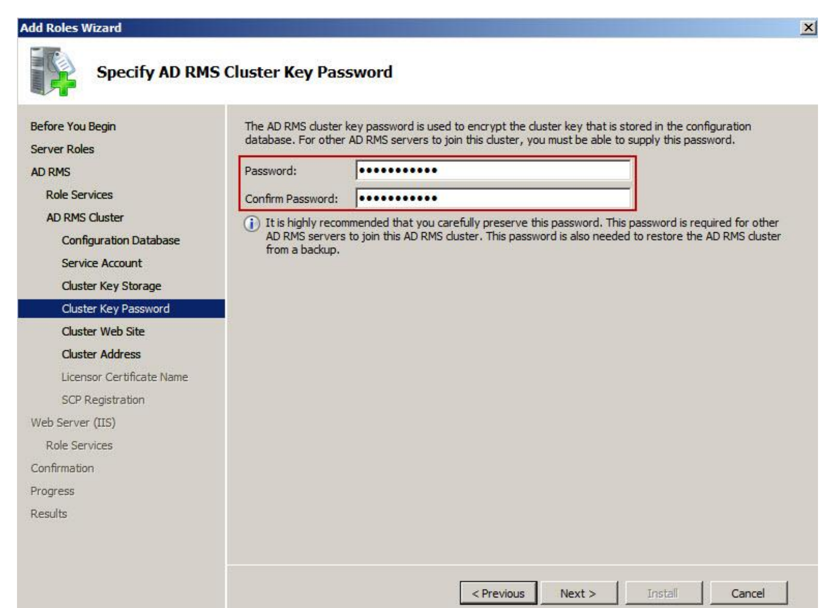
اذا كان هناك DB Server سنختار الاختيار الاخر
ولكننا سنستخدم الWindows Internal DB



نقوم بكتابه اسم وكلمه مرور الUser الذي تم انشاءه للتحكم في هذه الخدمه



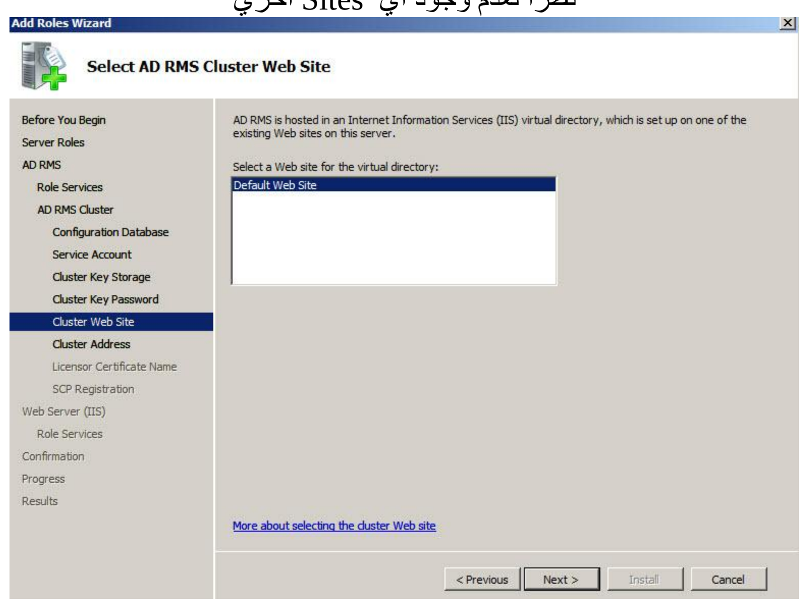
هنختار الkey AD RMS حتي لا يحدث أي Error



كلمه المرور الخاصه بهذه الخدمه

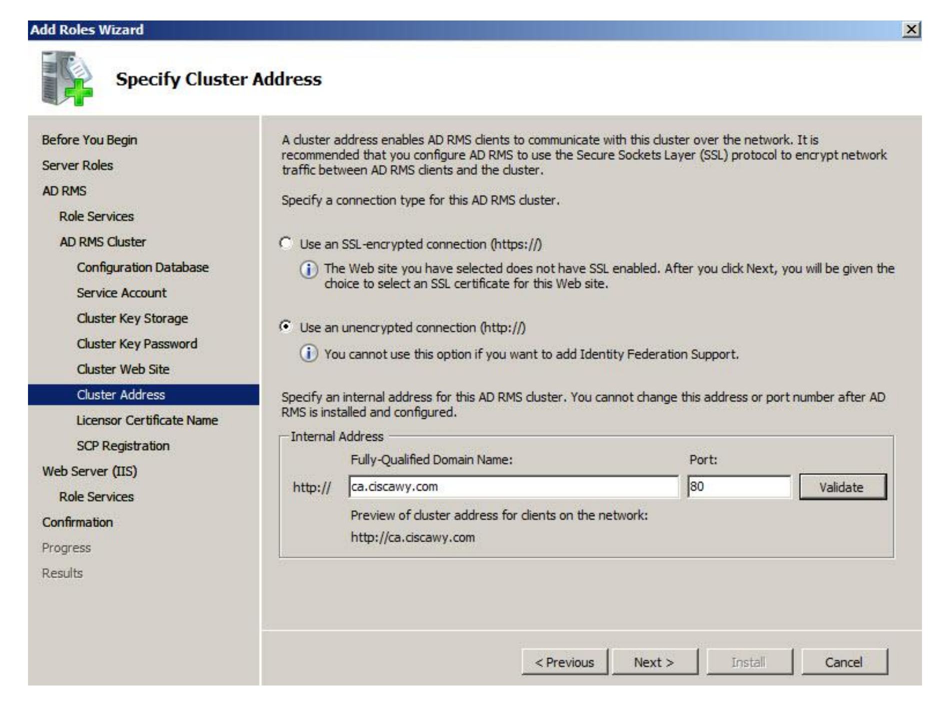
سنقوم باستخدام الDefault Web Site

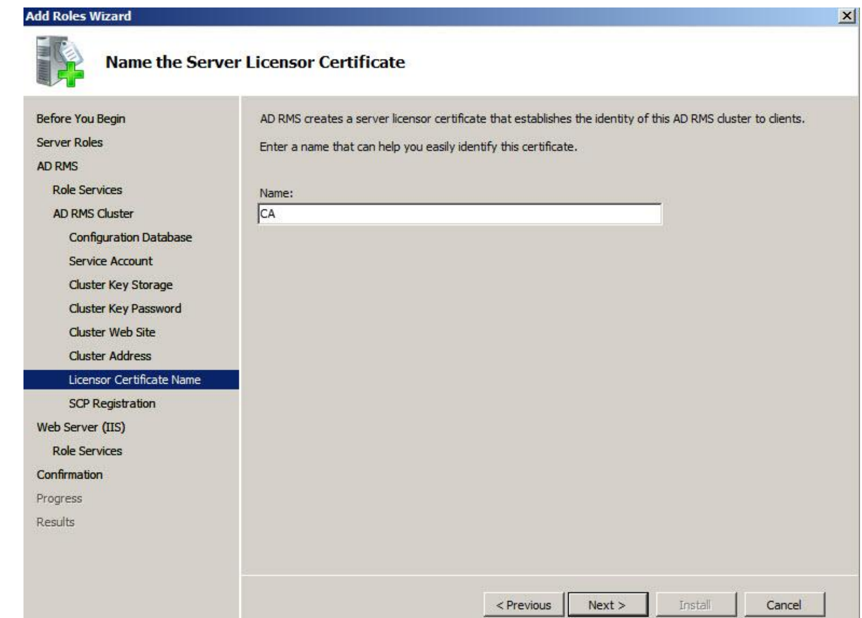
نظرا لعدم وجود اي Sites اخري



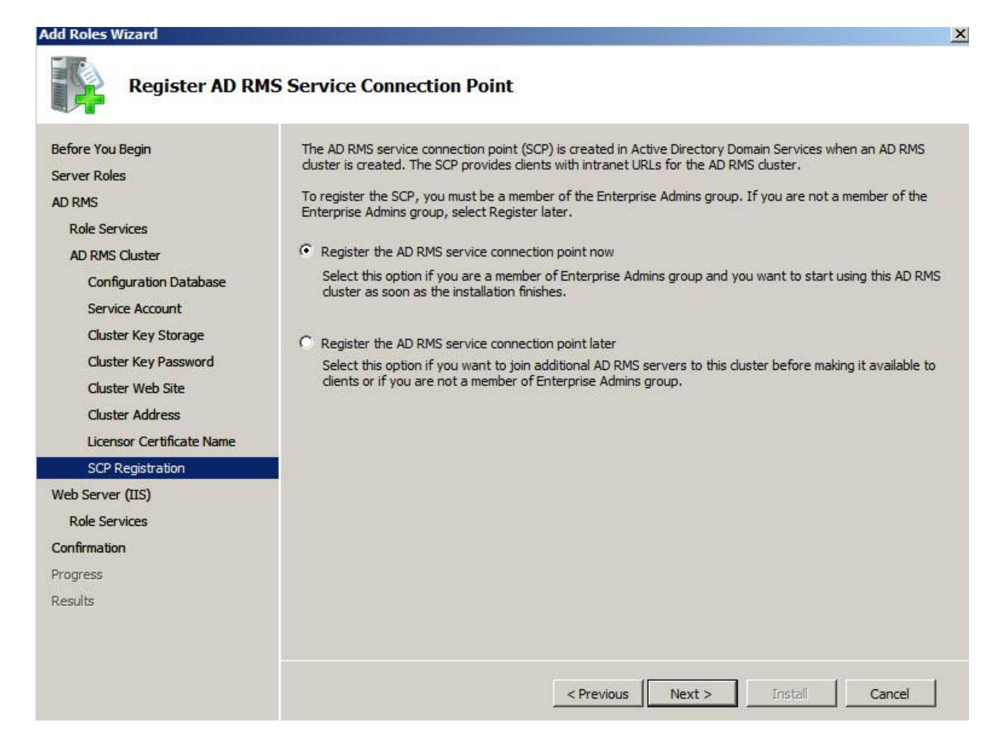
نحدد هل سنقوم بإستخدام HTTP or HTTPS

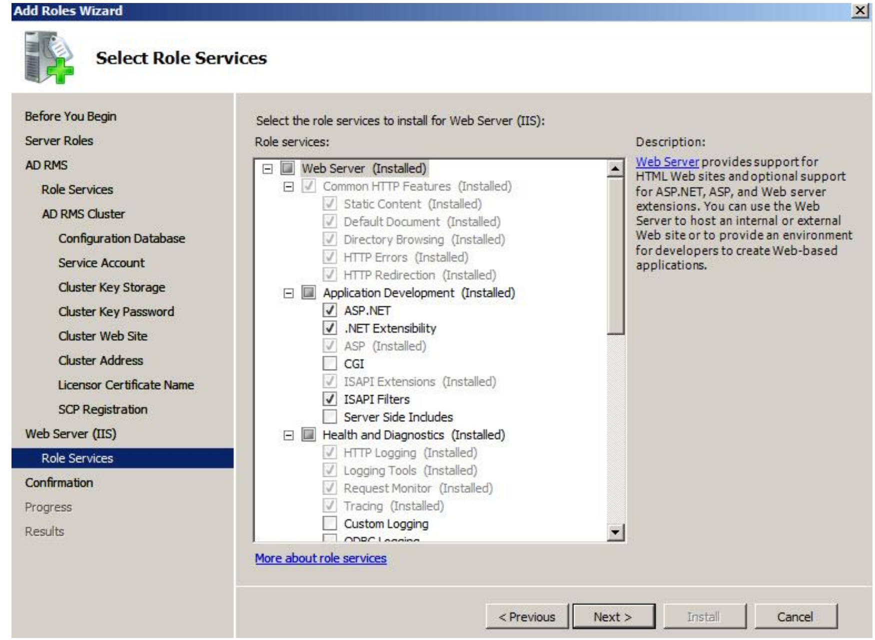
ونضيف اسم الMachine





طالما نحن نستخدم صلاحيات الEnterprise Administrator
نقوم بإنشاء الPoint الجديده





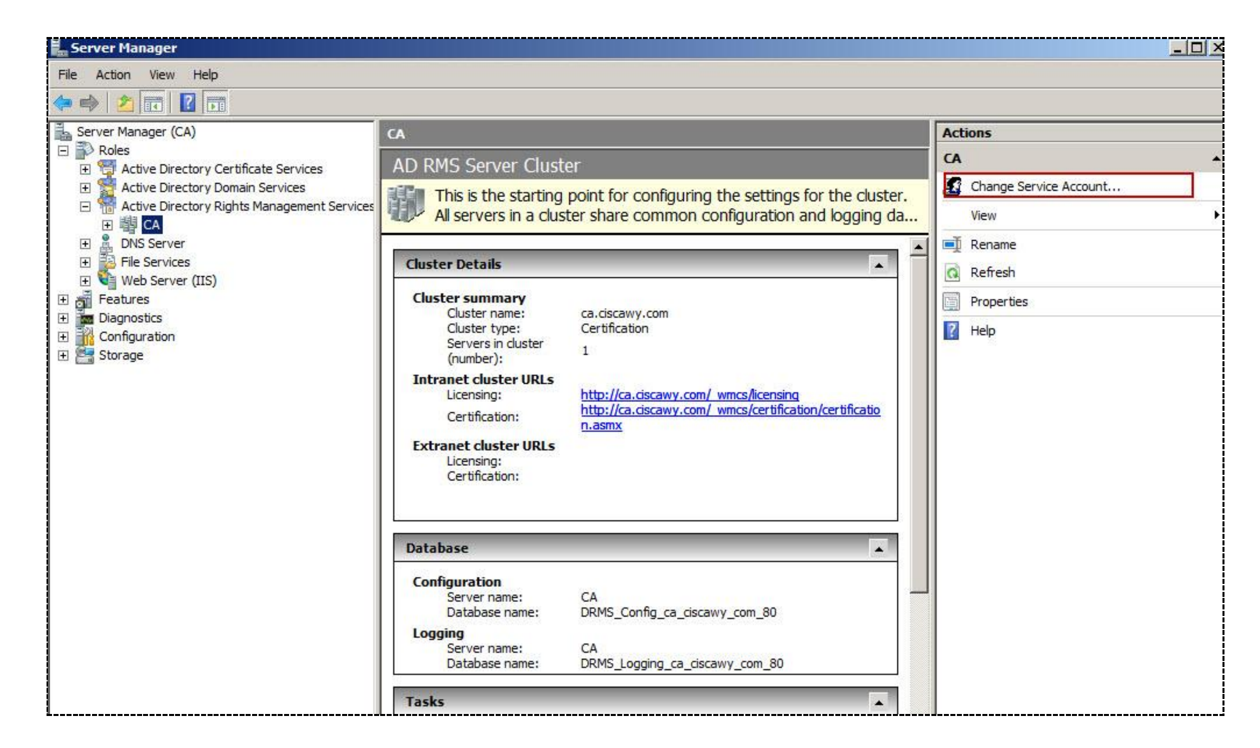
Install → Finish

بعد ذلك يجب ان نقوم بعمل Restart للServer

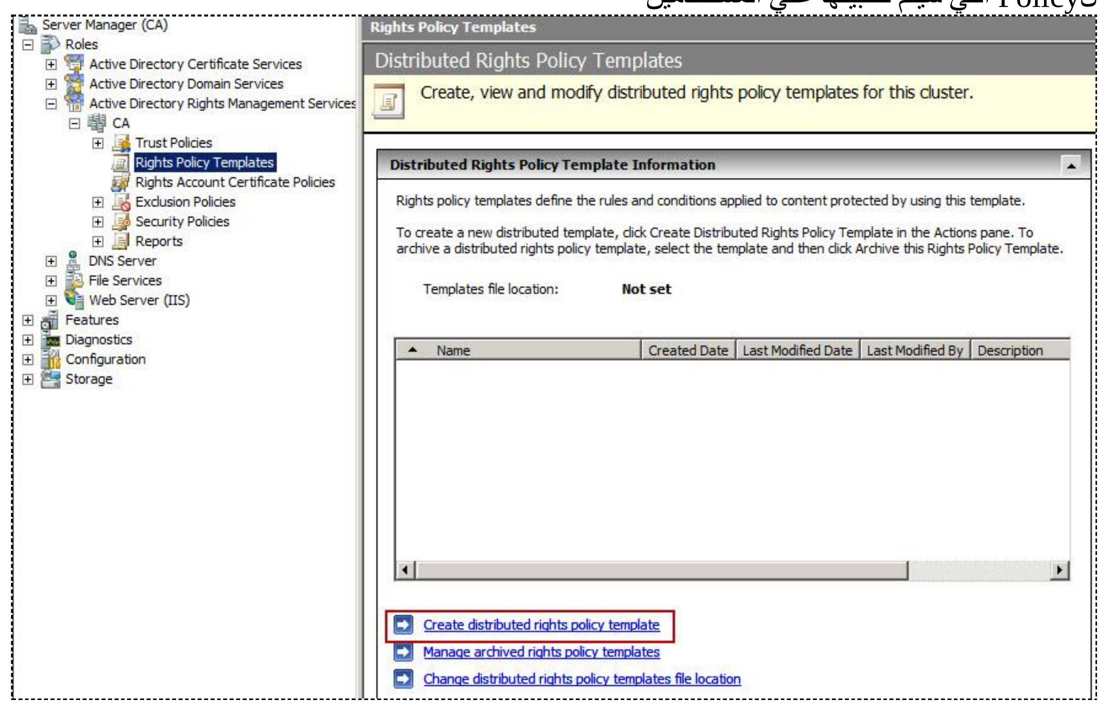
- نقوم بفتح الServer Manager

نختار AD RMS

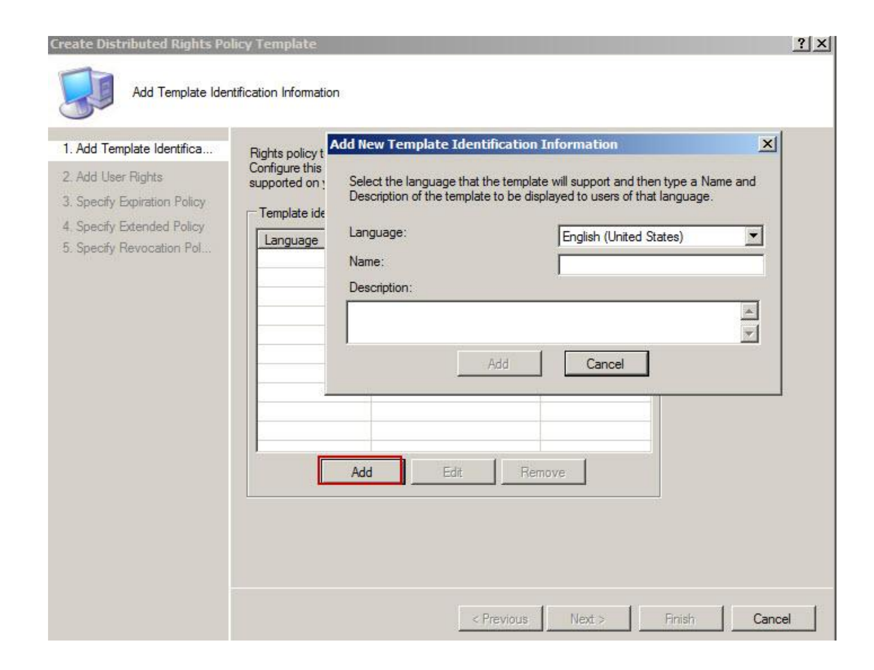
نلاحظ وجود Change Service Account من هذه الخدمه يمكن ان نقوم بتغيير اسم الUser المسئول عن هذه الخدمه الذي تم اضافته في الاعدادات الاوليه



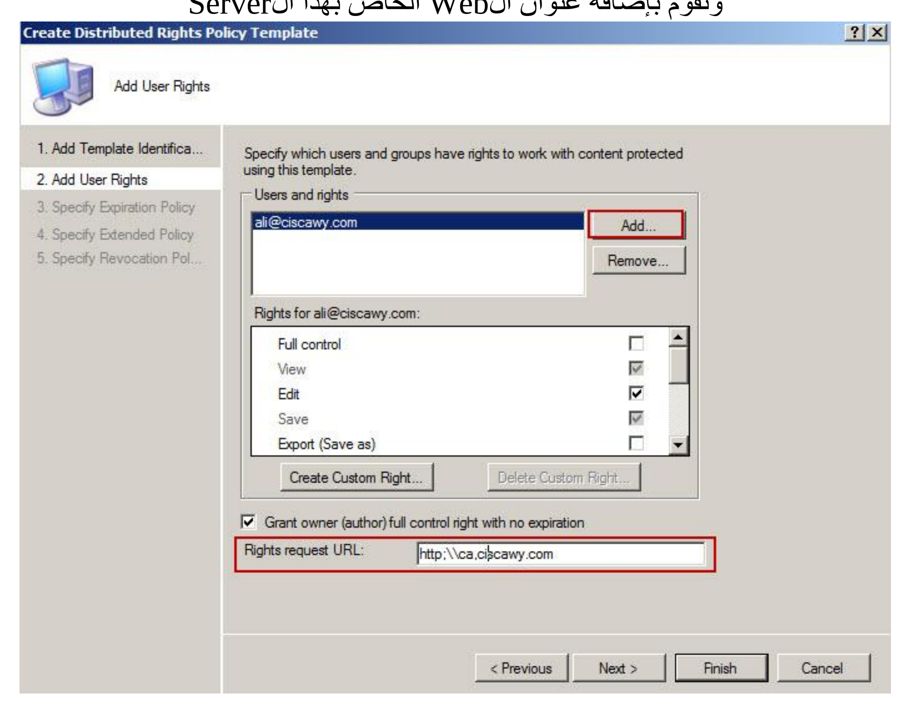
نختار Rights Policy Template
ومنها Cerate Distributed Rights Policy
هذه الPolicy التي سيتم تطبيقها علي المستخدمين



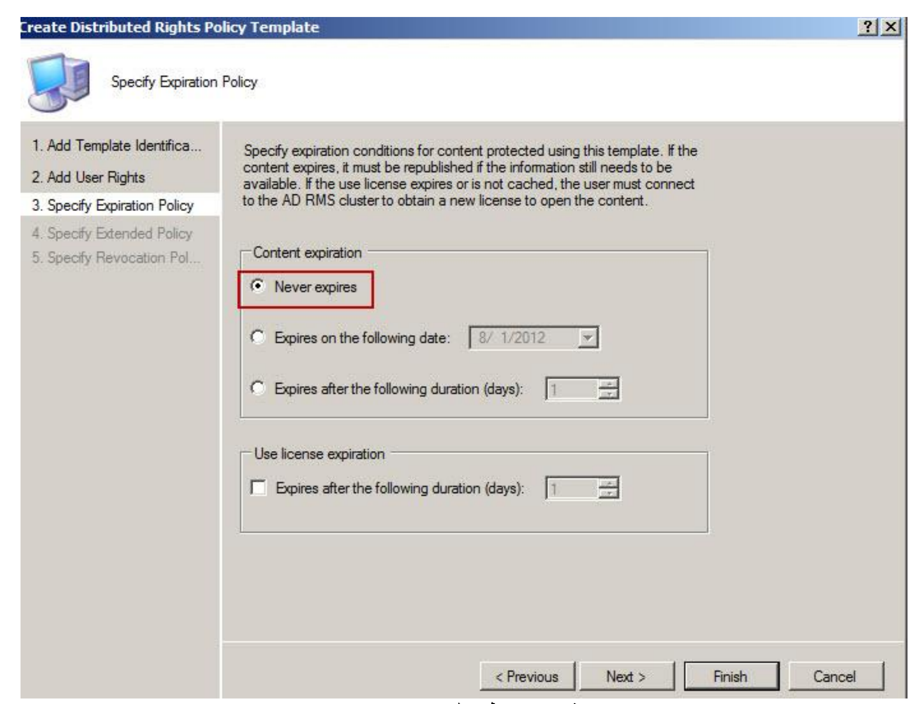
نضغط علي Add ونقوم بإضافه اسم ووصف لها



نضغط علي Add حتي نستطيع ان نضيف الUsers أو الGroups التي نريد تطبيق هذه الPolicy عليهم
نختار ايه المصرح بعمله
ونقوم بإضافه عنوان الWeb الخاص بهذا الServer



تحديد مده صلاحيه هذه الPolicy

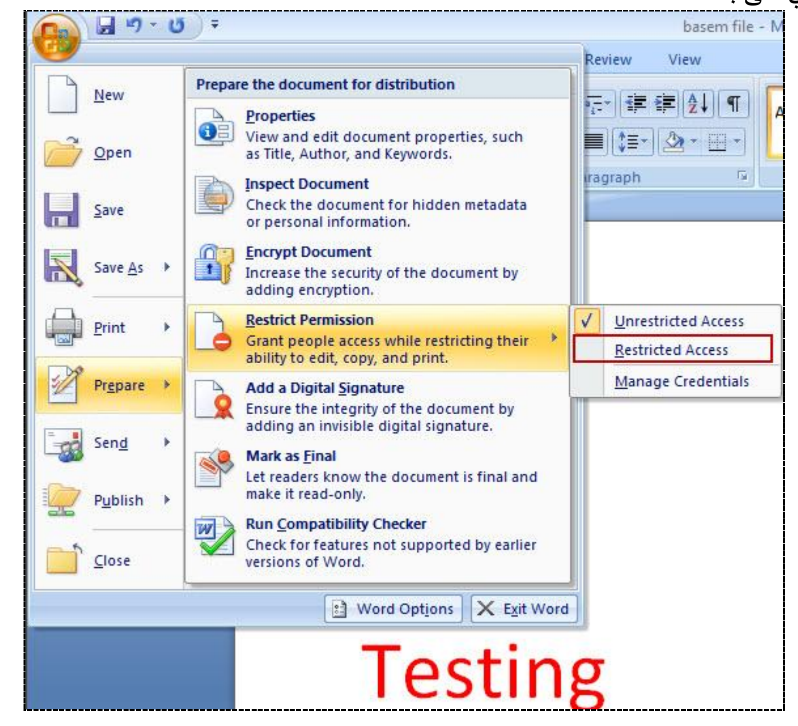


ثم نضغط علي Finish

- نقوم بعمل Shared Folder علي هذه الMachine
- ونقوم بتنزيل Microsoft office 2007\2010 علي جهاز الClient

- نقوم بالدخول علي Win-7

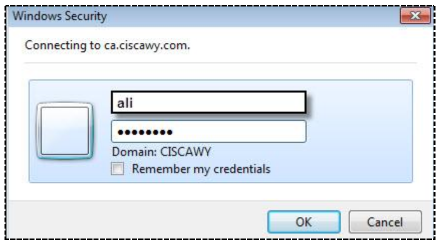
ندخل بحساب الUser الذي تم اضافته في الDistributed Rights Policy
نقوم بإنشاء ملف Word في الShared Folder
نقوم بفتحه وكتابه اي شئ به



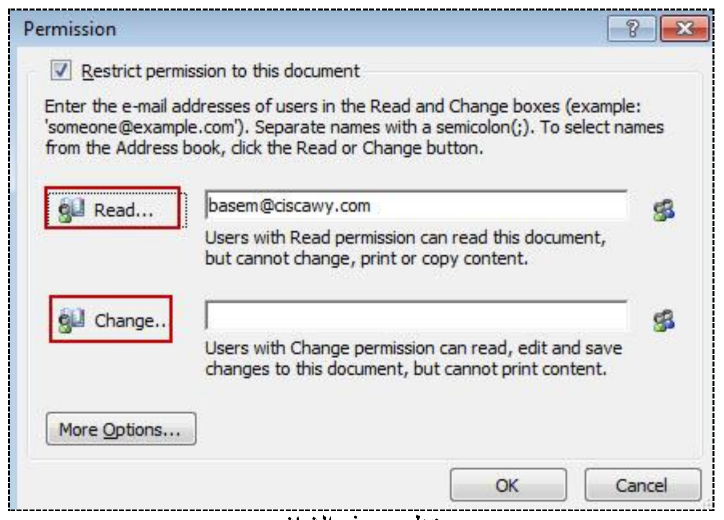
ثم نقوم بالضغط علي File → Prepare → Restrict policy → Restrict Access



سيقوم بالتأكد من الاتصال بخدمه الRMS



سيقوم بالسؤال عن صلاحيات هذا الUser



ستظهر هذه الشاشه
التي منها يتم تحديد صلاحيات المستخدمين الأخري لهذا الملف
يمكن ان تضغط علي Read وتضيف مستخدمين للقراءه فقط
و Change وهم من يمكنهم التعديل
More Option تضيف لهم صلاحيات اخري

ولكن شرط اساسي ان يكون لهؤلاء المستخدمين E-mail يتم اضافته في الAttributes الخاصه بهم

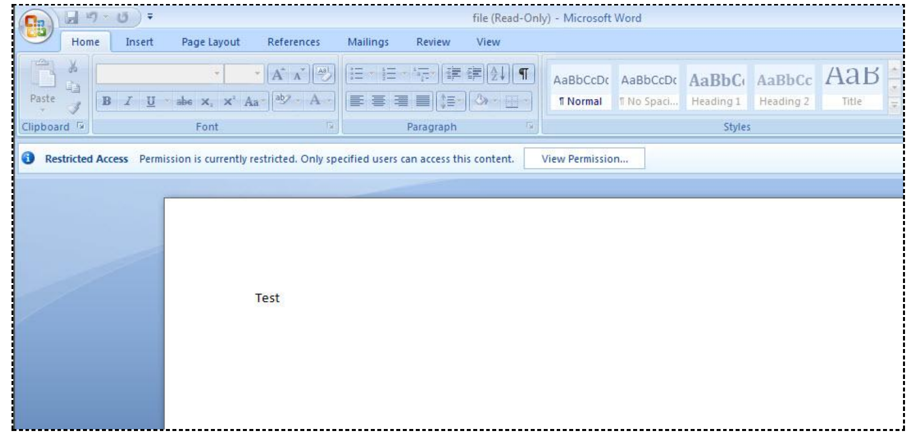
بعد ذلك نقوم بالدخول بصلاحيات المستخدم Basem حيث انه تم اعطاءه Read
نقوم بفتح الملف من علي الShared Folder
ستظهر هذه الرساله



تفيد ان هناك Permission تم تطبيقها علي هذا المستخدم

بعد فتح الملف ستجد انه ليس هناك اي Active Menu يمكن التعديل بها

وهو ملف للقراءه فقط



وان قمت بنقل الملف الي مكان آخر ستجد ايضا نفس هذه الصوره

مبروك عليك تم حمايه الملف الخاص بك بنجاح

Active Directory Federation Service

- إحدي الخدمات الجديدة المقدمه في Windows Server 2008
- وهي تعتبر بديلا عن موفوع الForest Trust
- أي لو أن هناك شركتان وأريد User من إحداهما A يقوم بـAccess Web Server مثلا أو Application معين نريد استخدامه علي الشركة الأخري B ،،

الشركتين في Forests مختلفه عن بعضهما

  - في الForest Trust لا بد ان يحدث Authentication من الفرعين حتي تتم عمليه الدخول
  - انما في الFederation Service تعتمد علي Single Sign On اي ان من اين منهما تحدث الوثوقية

- مميزات خدمة الFederation Service :-
  - تسهيل عملية الدخول والخروج الAuthentication
  - التحكم فيما يستطيع اي مستخدم ان يتعامل مع علي الفرع الآخر (التحكم في الخدمات المتاحة)
  - متوافق مع الADLDS و الADDS

- AD Federation Service Terms بعض المصطلحات الهامة التي سنتعامل معها :-
  - Resource Organization :-

الشركة او الفرع او الForest التي تحتوي علي الApplication المراد الوصول اليه

  - Account Organization

المستخدمين الموجودين في الفرع الآخر المراد السماح لهم للوصول للApplication
يمكن ان نستخدم الADLDS و الADDS

  - Federation Service :-

الخدمة التي ستقوم بعملية الربط بين الاثنين

- Claims :-

تحتوي علي المعلومات الخاصة بكل Domain
الأسم الصلاحيات الخدمات و هكذا

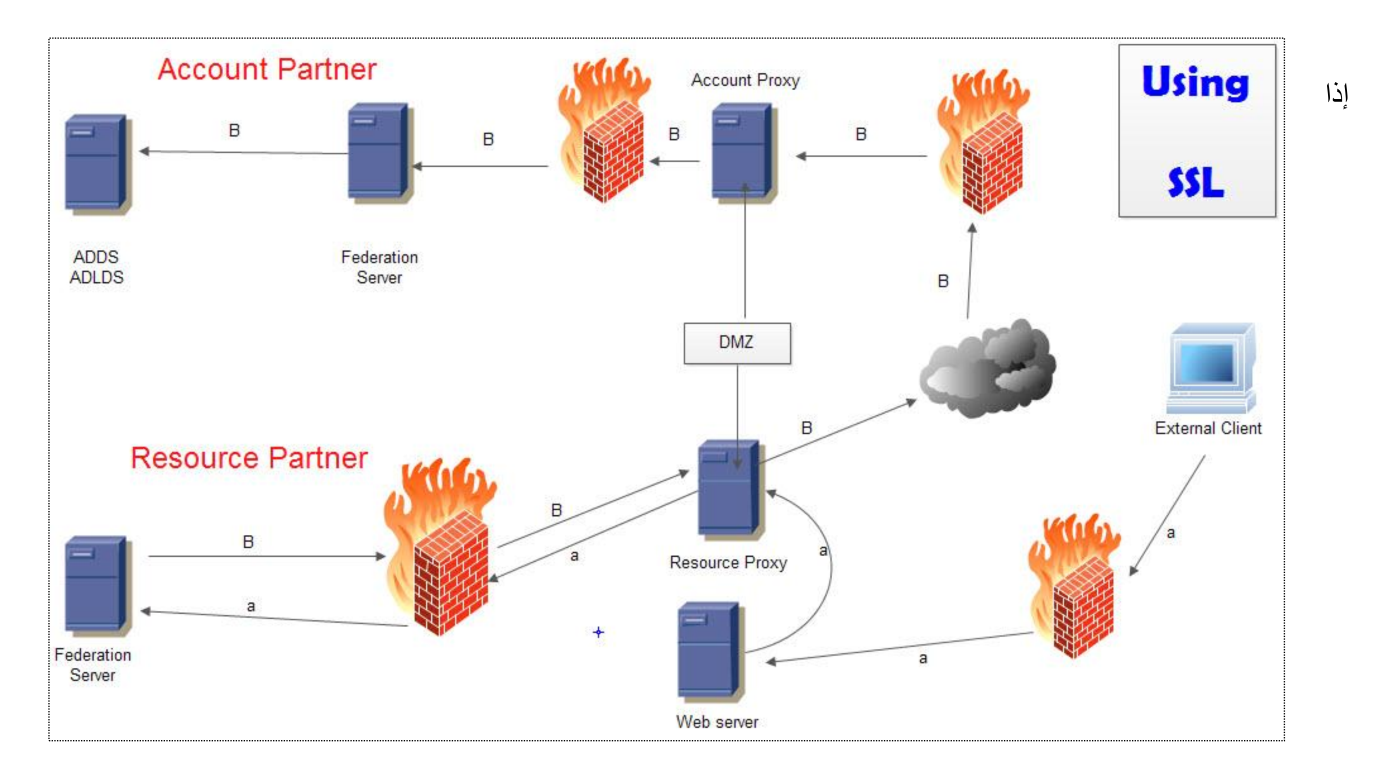
  - Claim aware :-

بحدد منه صلاحيات الAccounts علي الForest الاخري

  - Cookies :

تستخدم في عملية الAuthentication
وتمنع عمليه الRe- Authentication نظرا لوخود خاصيه الSingle Sign On

إذا



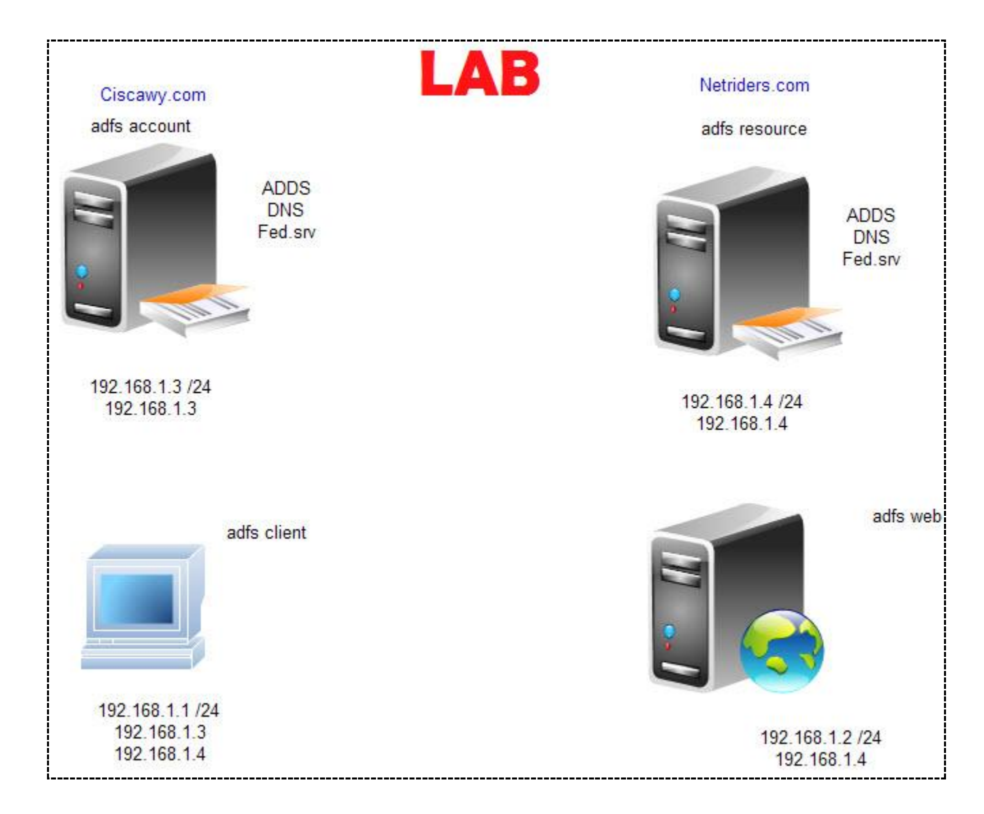
أراد الExternal Client الدخول علي الWeb server عليه أولا ان يتم السماح له من الResource Proxy وحيث انه لا يملك اي معلومات سيتم الاتصال بالFederation Server كما في المسار a مرورا بالFirewall سيتم اعاده ارسال الاتصال كما في المسار B الي الFederation Server الآخر ثم بالADDS للحصول علي الAuthentication الخاص بالمستخدم للدخول الي الWeb Server

لتطبيق هذه الخاصيه اتبع الScenario التالي :-

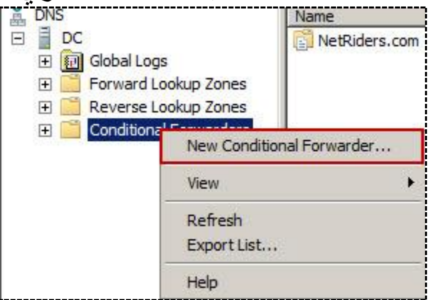
- سنحتاج الي 4 Machines
- اثنين Forest مختلفين Ciscawy.com و Netriders.com
- Machine مسئوله عن الWeb Server وهي Member of Netriders.com
- جهاز الClient العادي وهو Member of Ciscawy.com
- اتبع الخطوات كما هو موضح في الشكل واذا تم تغيير أين منهما اثناء التطبيق فعدله من الخطوات كما سنري سويا

- أسماء الـ Machines

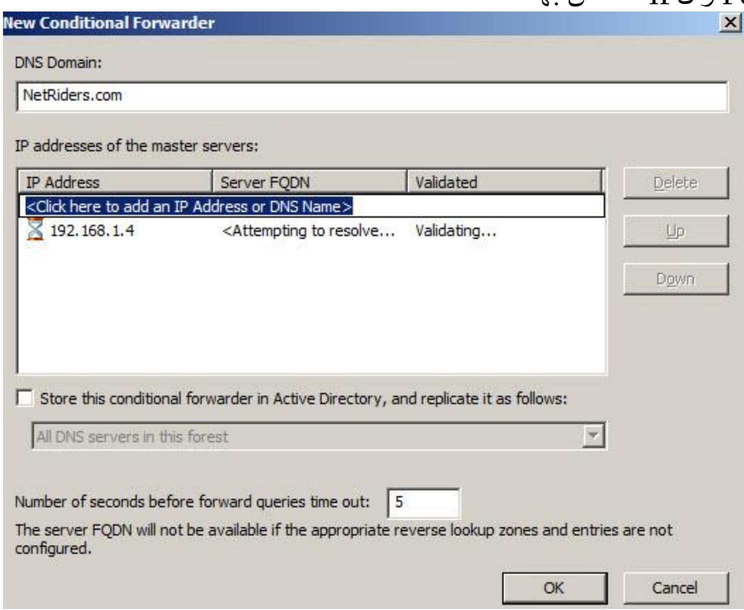
DC.ciscawy.com أول Forest Ciscawy.com
Resource.Netriders.com الForesf الاخري Netriders.com
Web.Netriders.com السيرفر المراد الدخول عليه Member of Netriders.com
Win-7.ciscawy.com جهاز الClient Member of Ciscawy.com



علي اول Forest Ciscawy.com
سنقوم بإنشاء User و Group سنستخدمهم في عمليه ال Authentication
نقوم بفتح الDNS لإنشاء Conditional Forward خاصه بالForest الاخري Netriders.com

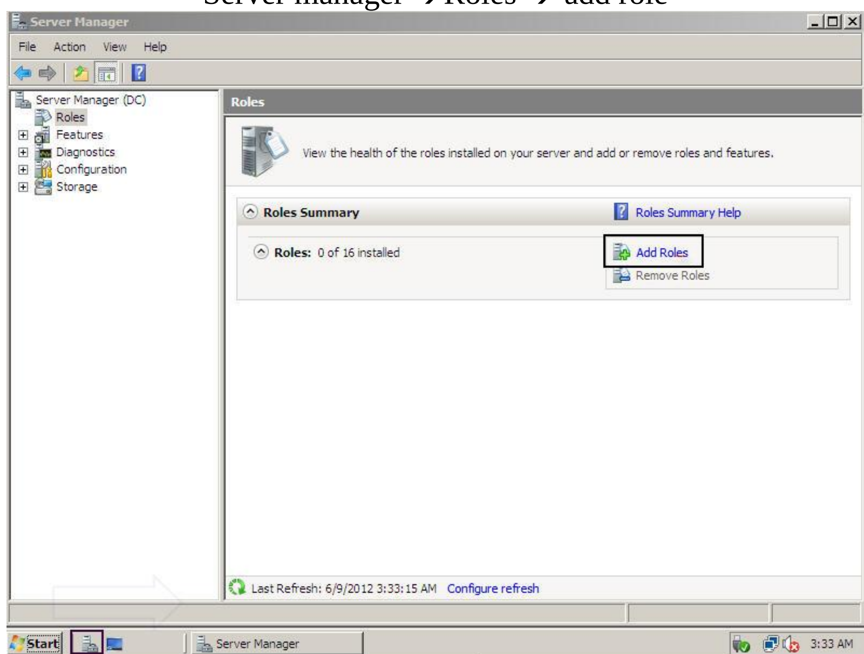


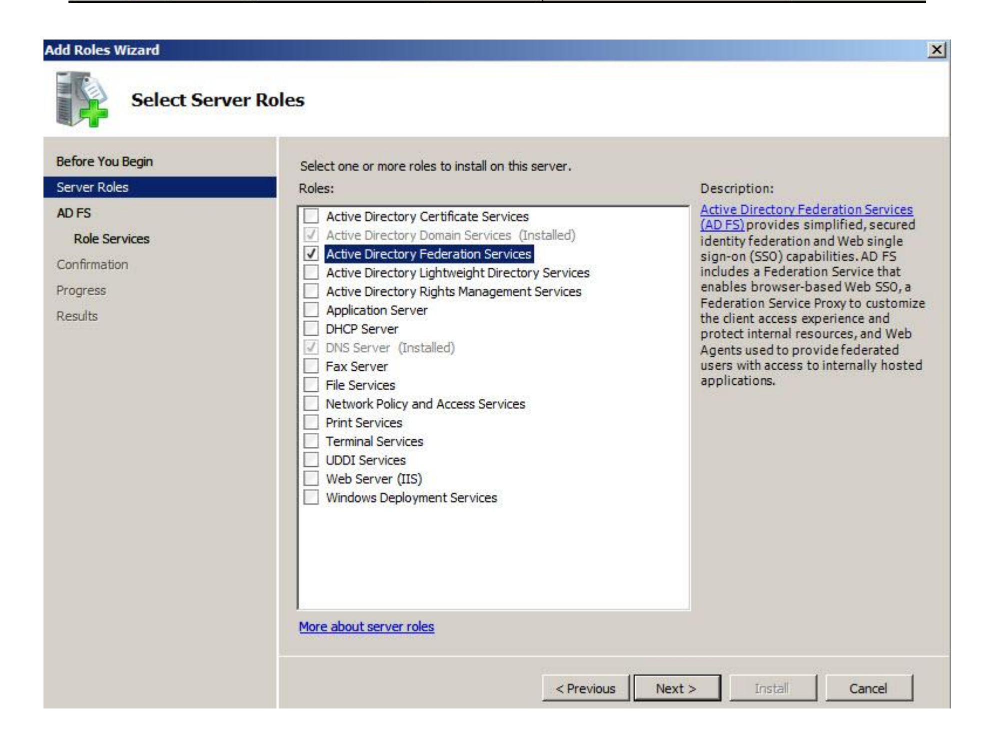
نقوم بإدخال اسم الForest والIP الخاص بها



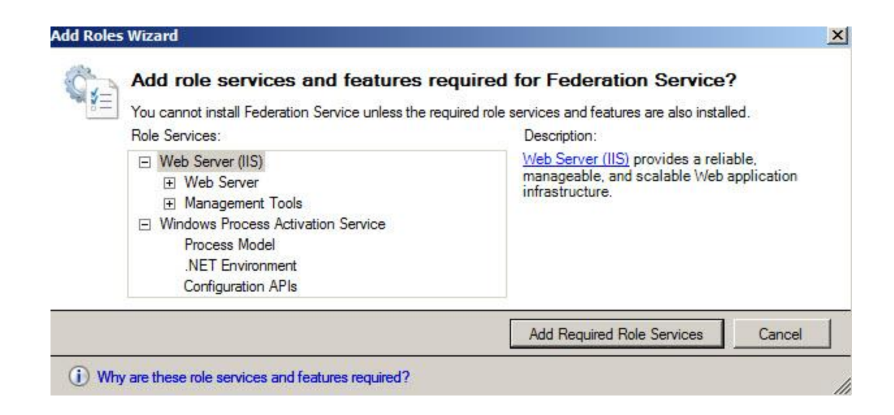
علي الForest الاخري Netriders.com
ونقوم ايضا بنفس الخطوات المتبعة في انشاء Conditional Forward خاصه بCiscawy.com

بعد ذلك نقوم بتصطيب خدمة ال**Federation** علي كل منهما
Server manager →Roles → add role





نقوم بتنزيل خدمه الIIS



نختار Create Self Sign Certificate
اي Certification داخليه سنحتاجها في عمليه الوثوقيه بين الTwo Forest

Add Roles Wizard

Choose a Server Authentication Certificate for SSL Encryption

Before You Begin
Server Roles
AD FS
Role Services
Server Authentication Certificate
Token-Signing Certificate
Trust Policy
Web Server (IIS)
Role Services
Confirmation
Progress
Results

When communicating with clients, AD FS uses the Secure Sockets Layer (SSL) protocol to encrypt network traffic. Choose a server authentication certificate suitable for SSL encryption to add to the default site in Internet Information Services (IIS).

Choose an existing certificate for SSL encryption (recommended)

This option is recommended for most production scenarios. You should use a certificate issued by an external certification authority (CA); or you can use a certificate issued by your own internal CA if the CA is trusted by clients connecting to this server. The subject name of the certificate must match the host name of this server.

Issued To	Issued By	Expiration Date	Intended Purpose

Properties
Import
Refresh

Create a self-signed certificate for SSL encryption

This option is recommended for small-scale deployments or test scenarios only. After installing AD FS, you must manually install the certificate on clients that communicate with this server.

More about choosing a certificate for SSL encryption

< Previous | Next > | Install | Cancel

Add Roles Wizard

Choose a Token-Signing Certificate

Before You Begin
Server Roles
AD FS
Role Services
Server Authentication Certificate
Token-Signing Certificate
Trust Policy
Web Server (IIS)
Role Services
Confirmation
Progress
Results

When the federation server issues a token to a client, it digitally signs the token using a token-signing certificate. When the client receives a token from the federation server, it uses the certificate to verify that the token was issued by the correct federation server and that the token has not been tampered with.

Choose the certificate to use for signing tokens issued by this federation server.

Choose an existing token-signing certificate (recommended)

This option is recommended for most production scenarios. You can use a certificate issued by your own internal certification authority (CA) if you have one; or you can use a certificate issued by an external CA.

Issued To	Issued By	Expiration Date	Intended Purpose

Properties
Import
Refresh

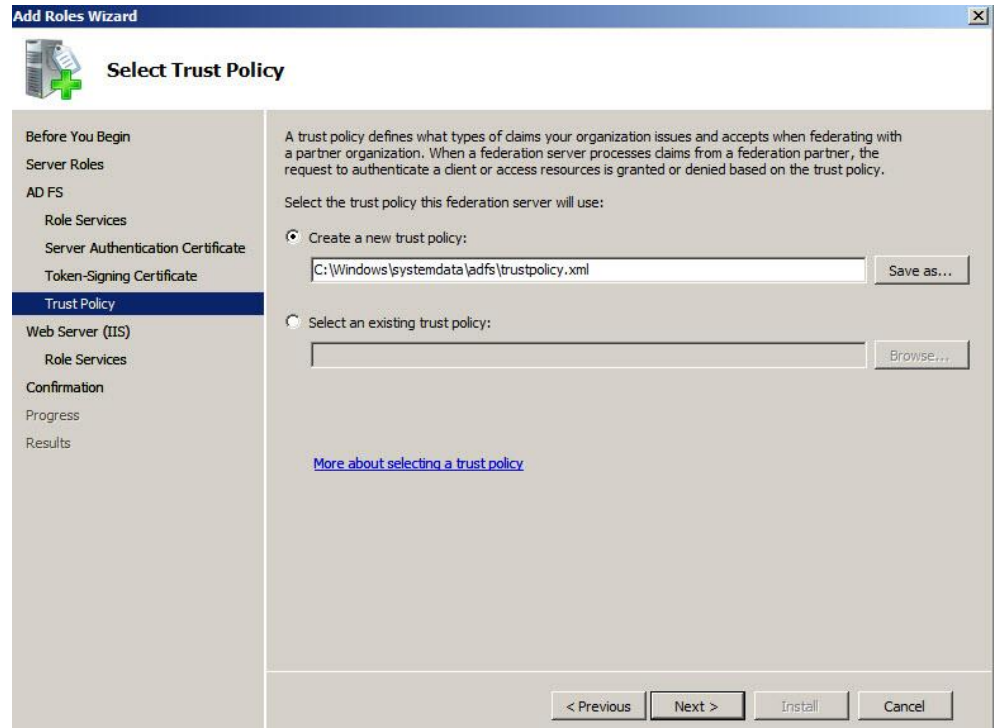
Create a self-signed token-signing certificate

This option is recommended if you don't have your own internal CA or don't want to use a certificate issued by an external CA. After installing AD FS, you must manually install the certificate on federation servers and federation service proxies that communicate with this server.

More about choosing a token-signing certificate

< Previous | Next > | Install | Cancel

نختار Create Trusted Policy



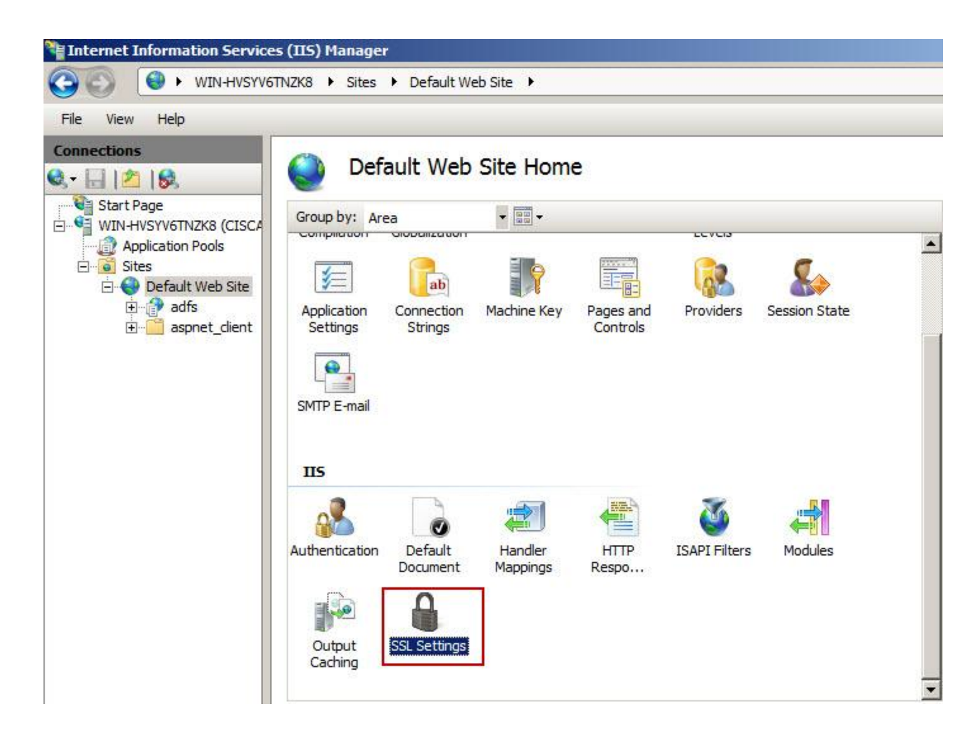
نترك اعدادات الIIS كما هي ثم نختار Next ثم Install

نفس الخطوات نقوم بإجراءها علي الForest الاخري

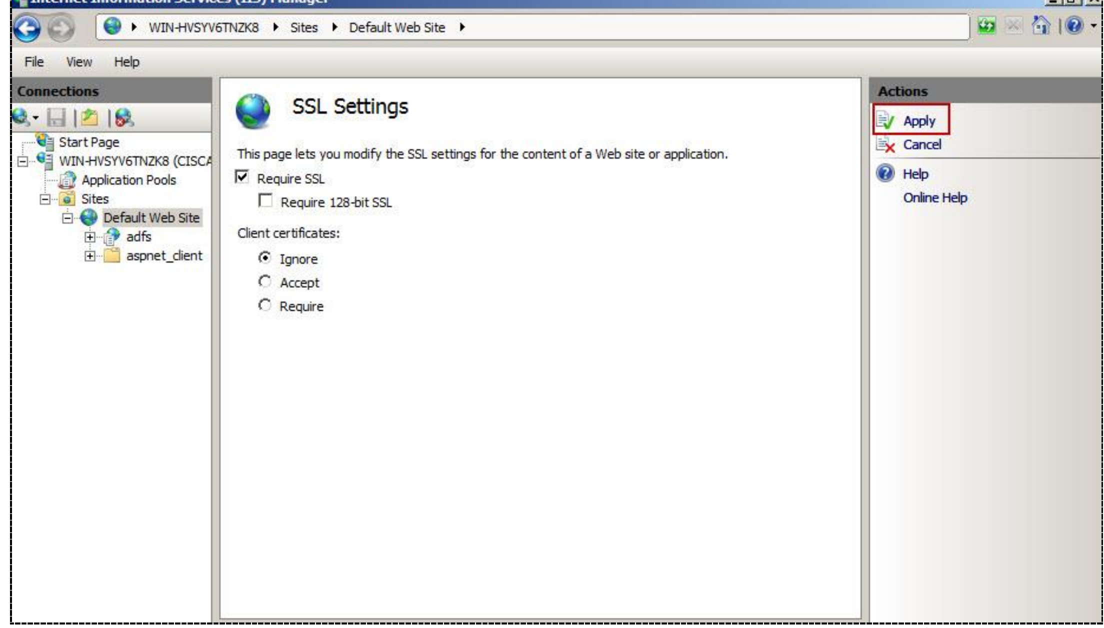
نقوم بإجراء بعض التعديلات علي الIIS أيضا علي كل منهما :-

Start → run → IIS

نفتح الDefault Web Site ونختار منها الSSL Setting



نضع ✓ علي Require SSL ثم Apply حتي يكون الاتصال مشفر بين الاثنين

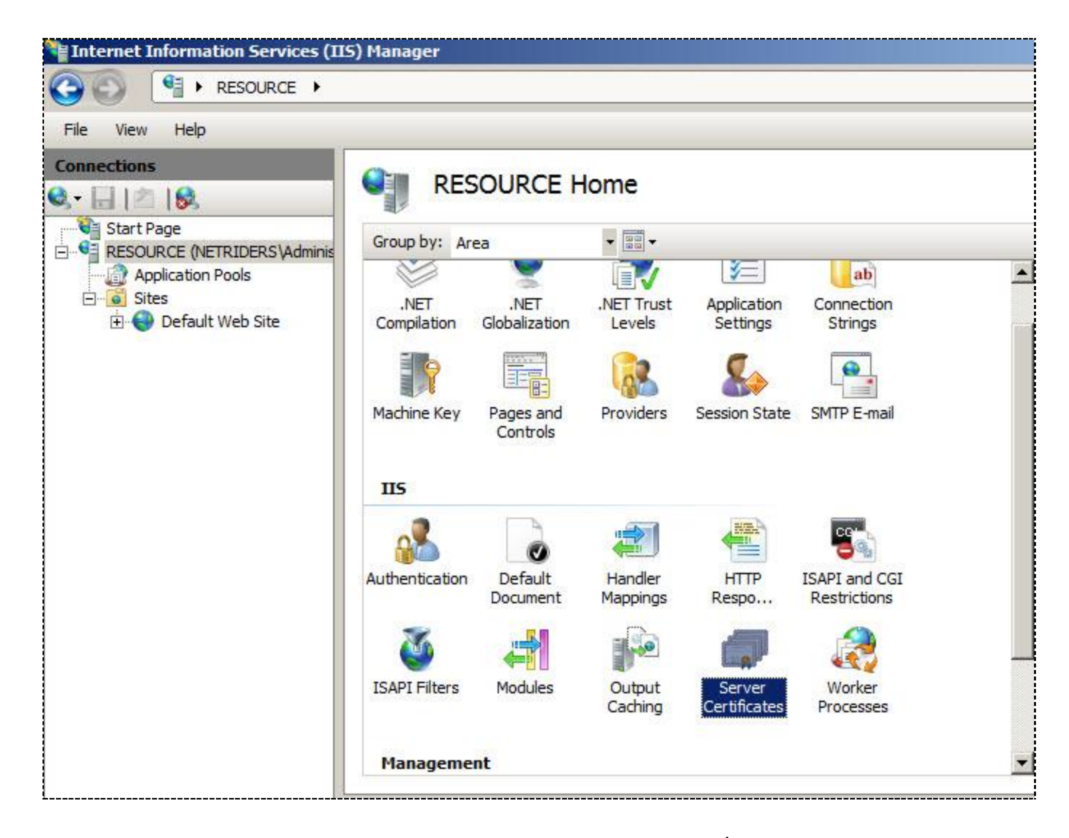


بعد الانتهاء من هذه الخطوه علي كل من الTwo Forest

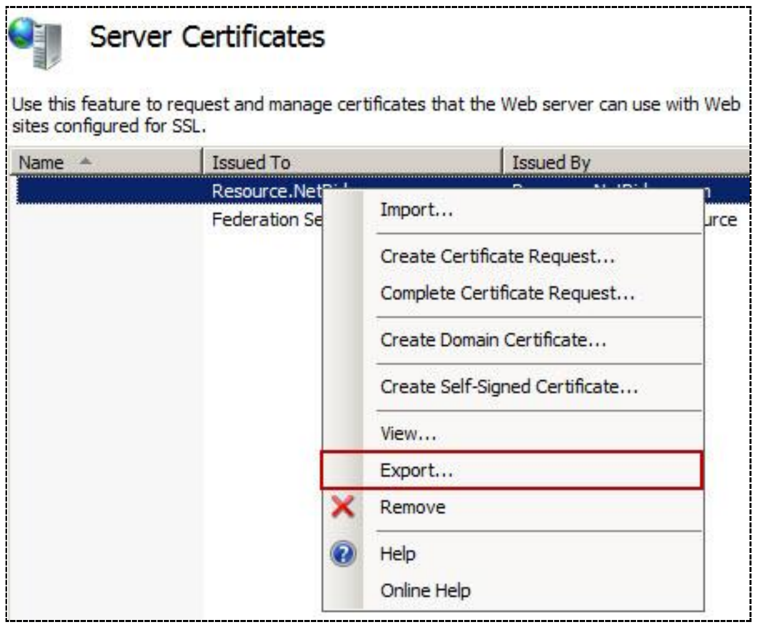
علي الForest الثانيه Netriders.com :-

نقوم بعمل Export للCertificate وبعد ذلك سنقوم بوضعها في الWeb Server

Start → run → IIS → Server Certificates

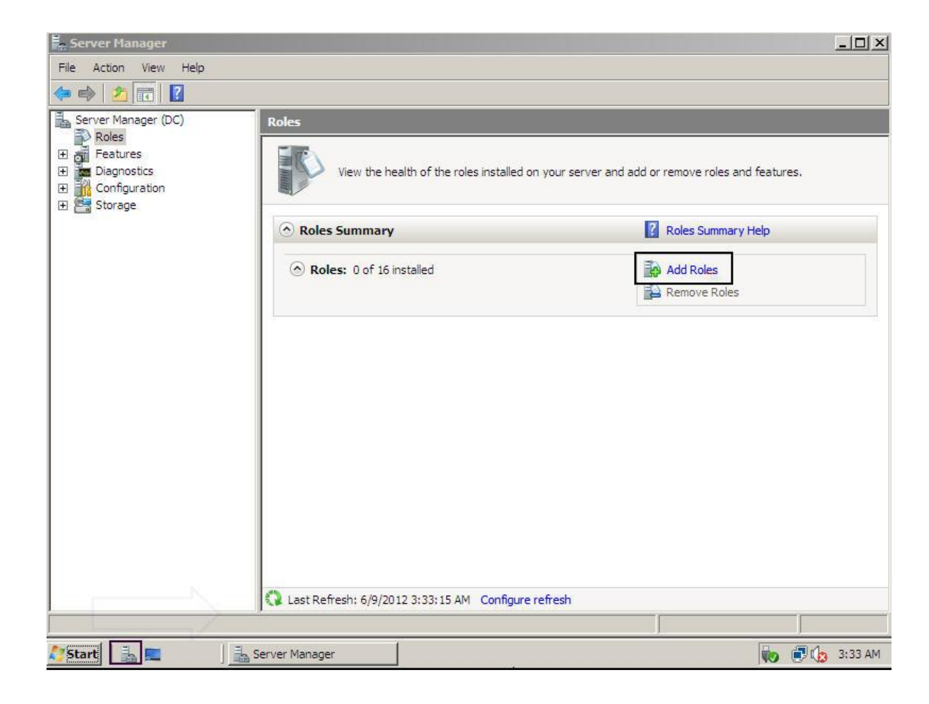


نقوم بالضغط عليها ونختار الResource أو المساه بإسم الMachine ونضغط R.click ثم Export ونختار مكان الحفظ



يتم حفظها
وسيتطلب منك ان تضع لها Password
يتم وضعها في Shared Folder لأننا سنستخدمها لاحقا

علي الMachine الثالثه التي تكون Member من Netriders.com
التي ستلعب دور الWeb Server
Server manager →Roles → add role



ونختار ايضا ACFS

Add Roles Wizard

Select Server Roles

Before You Begin
Server Roles
AD FS
Role Services
Confirmation
Progress
Results

Select one or more roles to install on this server.
Roles:

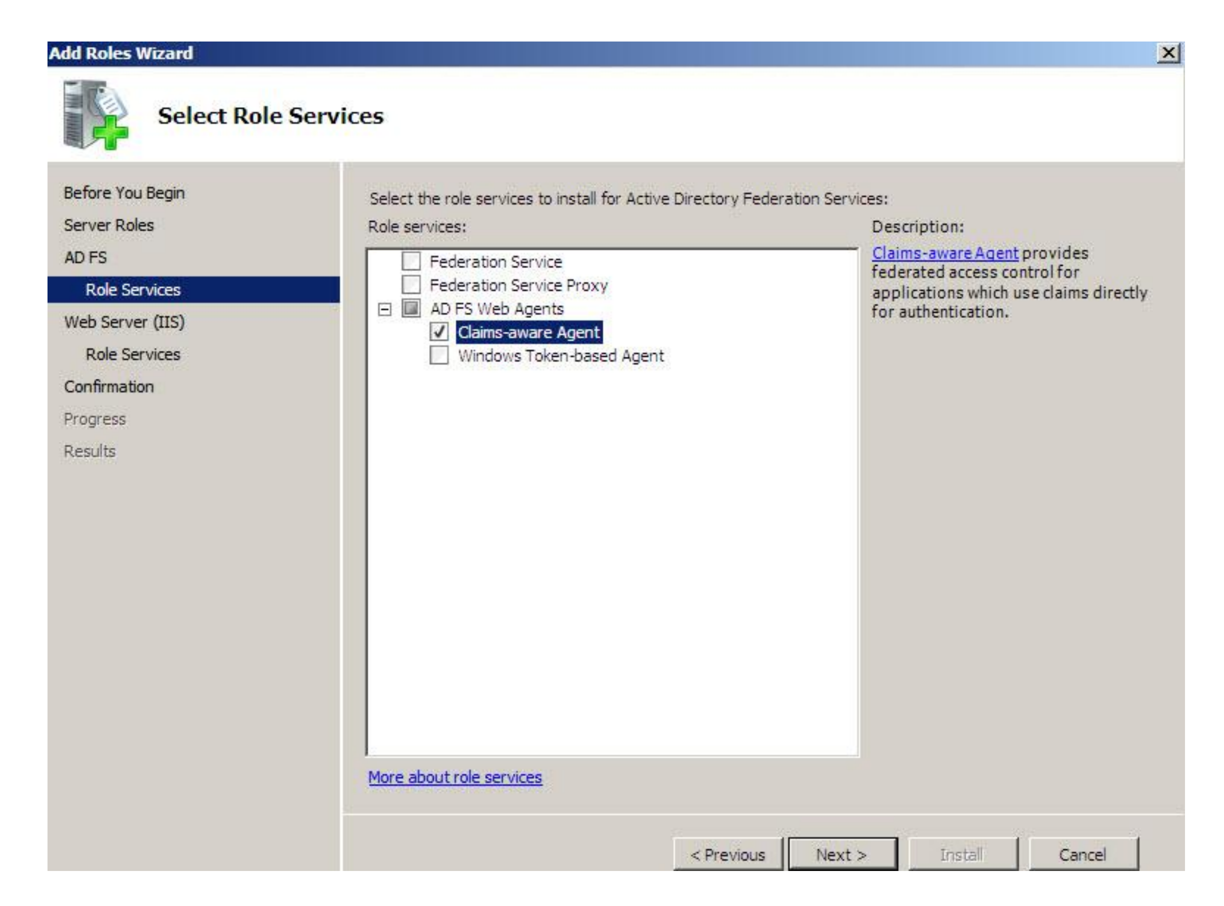
- [ ] Active Directory Certificate Services
- [ ] Active Directory Domain Services
- [x] Active Directory Federation Services
- [ ] Active Directory Lightweight Directory Services
- [ ] Active Directory Rights Management Services
- [ ] Application Server
- [ ] DHCP Server
- [ ] DNS Server
- [ ] Fax Server
- [ ] File Services
- [ ] Network Policy and Access Services
- [ ] Print Services
- [ ] Terminal Services
- [ ] UDDI Services
- [ ] Web Server (IIS)
- [ ] Windows Deployment Services

Description:
Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. AD FS includes a Federation Service that enables browser-based Web SSO, a Federation Service Proxy to customize the client access experience and protect internal resources, and Web Agents used to provide federated users with access to internally hosted applications.

More about server roles

< Previous | Next > | Install | Cancel

هنا سنختار الClaim aware agent فقط
لأن هذه هي التي سيقوم الClient بالدخول Access عليها



ينقوم أيضا بتنزيل الIIS



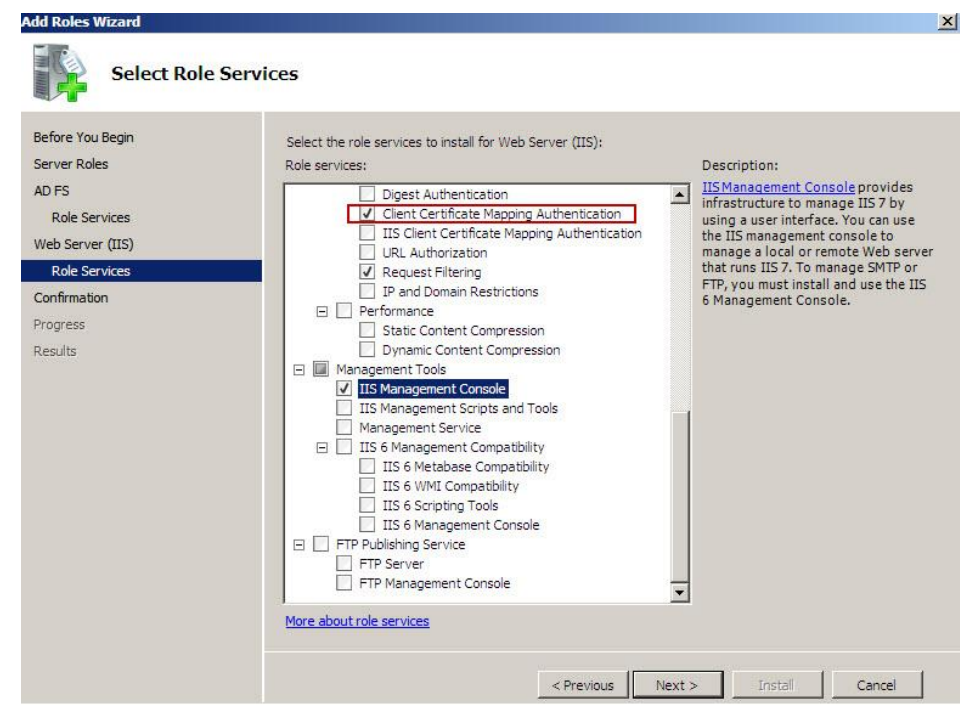
Next

سنختار هنا اضافه :-

Client Certificate mapping authentication

IIS management console

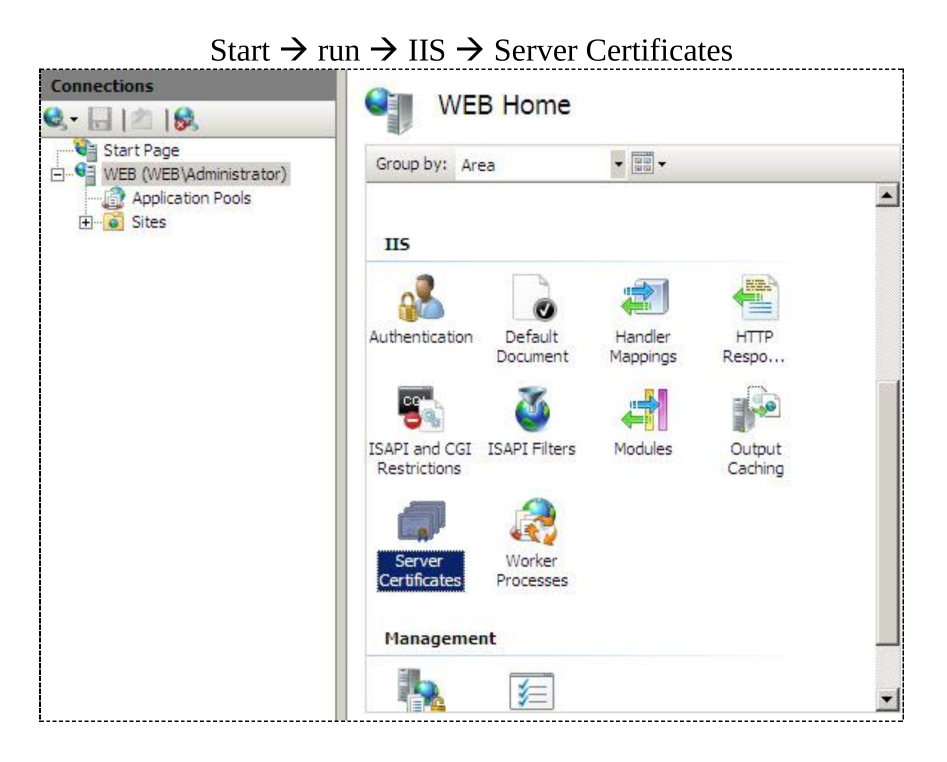
كما هو موضح



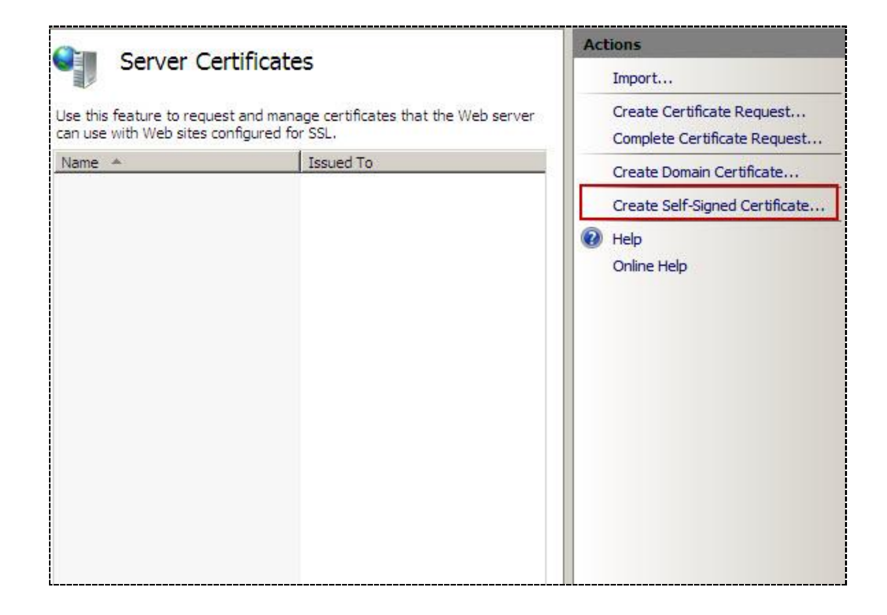
Next → Finish

علي نفس الMachine نقوم بفتح الIIS لإنشاء Self Sign Certificate

Start → run → IIS → Server Certificates



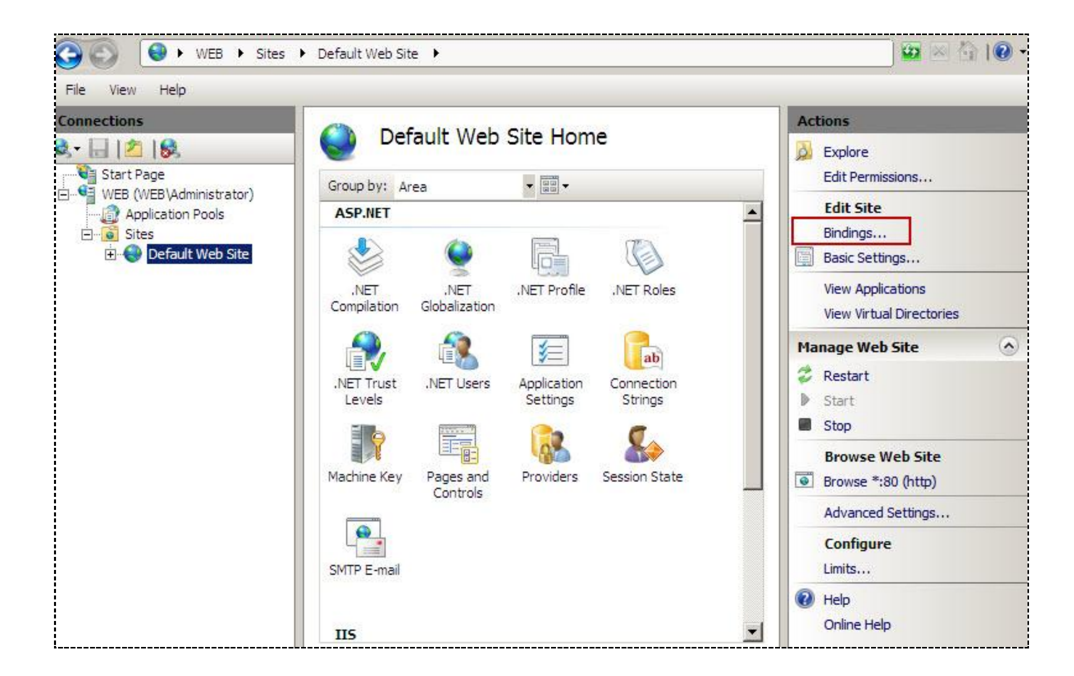
نختار من علي اليمين Create Self-Sign Certificate



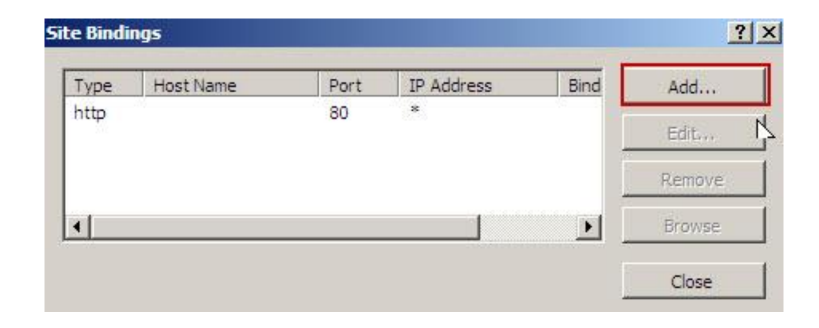
نختار اسم لها



بعد ذلك نقوم بفتح الSites ← Default web site
نختار Binding من علي اليمين



نضغط علي Add

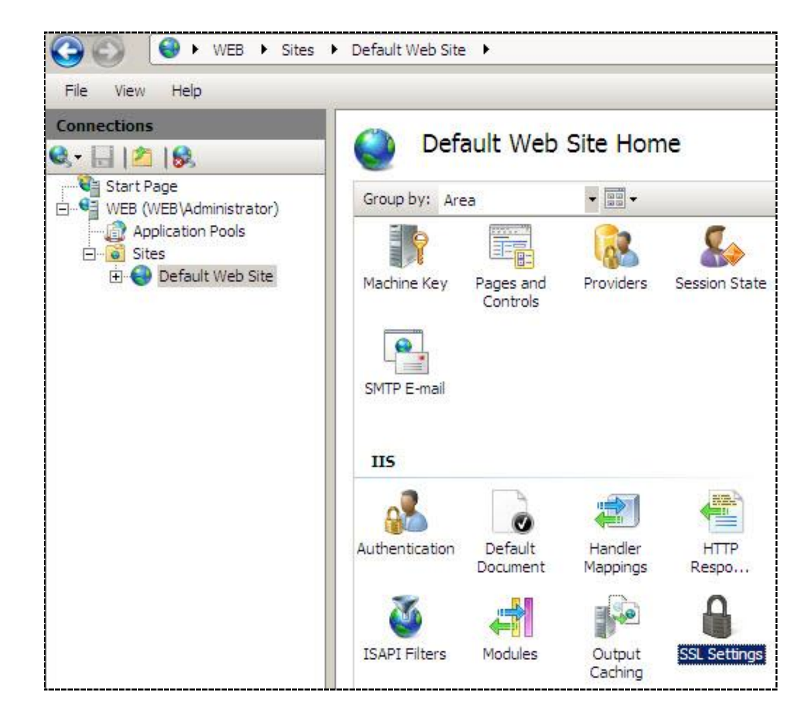


نختار الType ويكون https حتي يكون مشفرا
ونختار الCertification التي تم انشاءها من قبل علي هذه الMachine

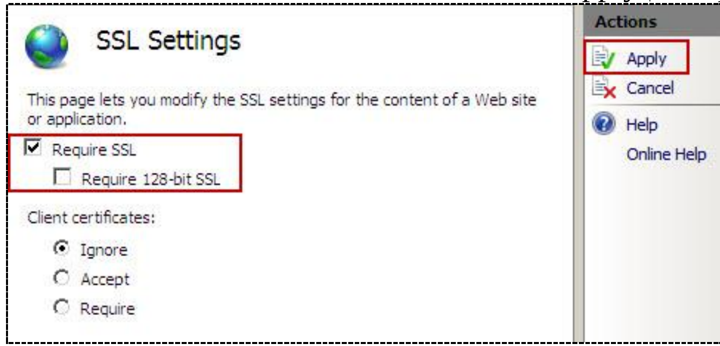


ثم نضغط علي OK

نقوم بتفعيل الSSl علي هذه الMachine أيضا

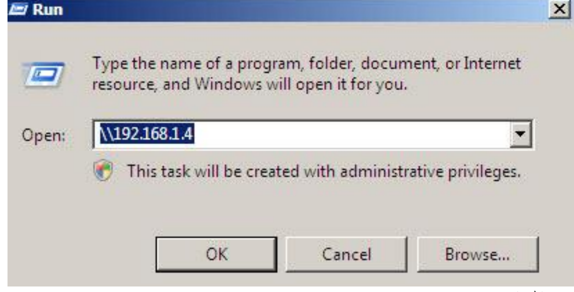


نضع ✓ علي Require SSL ثم Apply



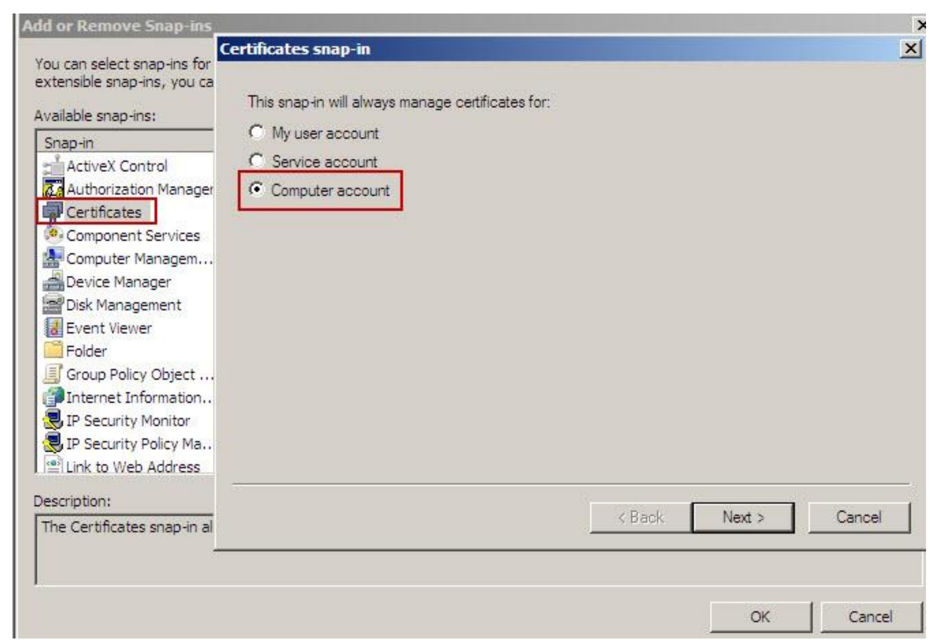
سيتم الآن عمل **Import** لل**Certification** التي تم تخزينها من علي Resource.Netriders.com :-
أهميتها انه يكون هناك اتصال بين الWeb Server و الFederation Server

يقوم بفتح المسار الخاص بهذه الMachine



يتم نسخ الCertificate علي سطح المكتب
ثم نقوم بفتح الMMC

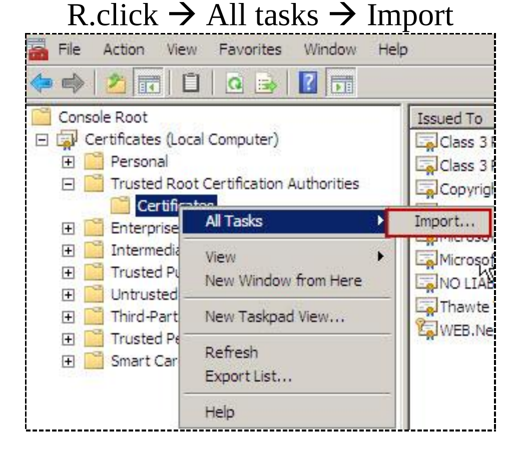
Start → run → MMC → File → add\remove snap in
نختار Certificate ونضغط علي Add



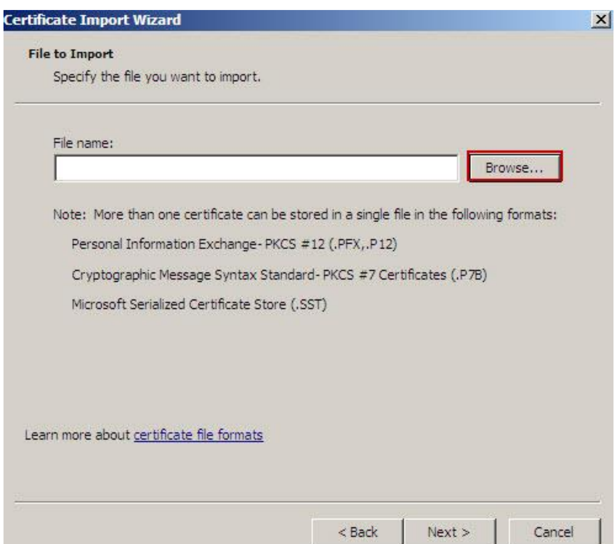
Next → Finish

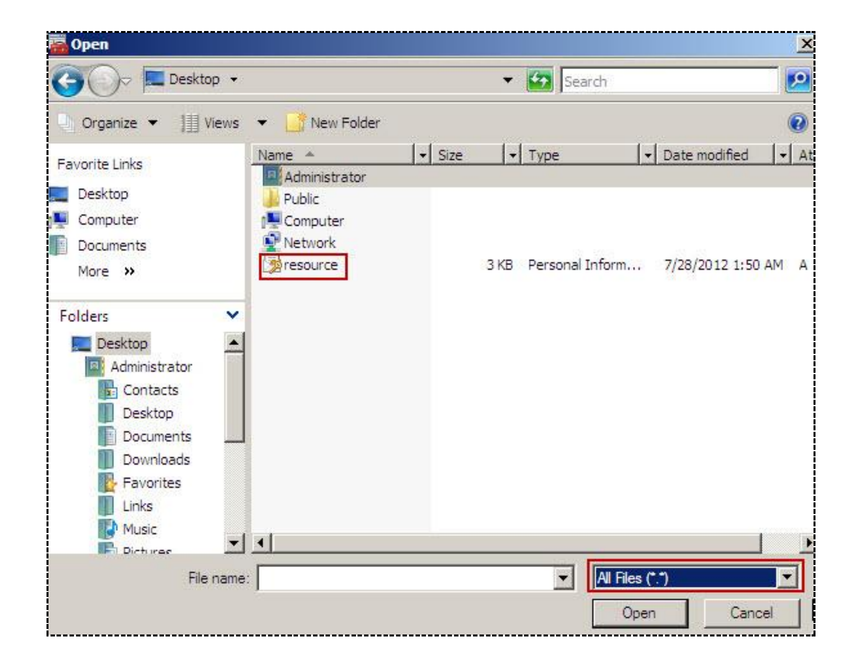
نقوم بفتحها ثم نختار Trusted Root ومنها Certificate

R.click → All tasks → Import

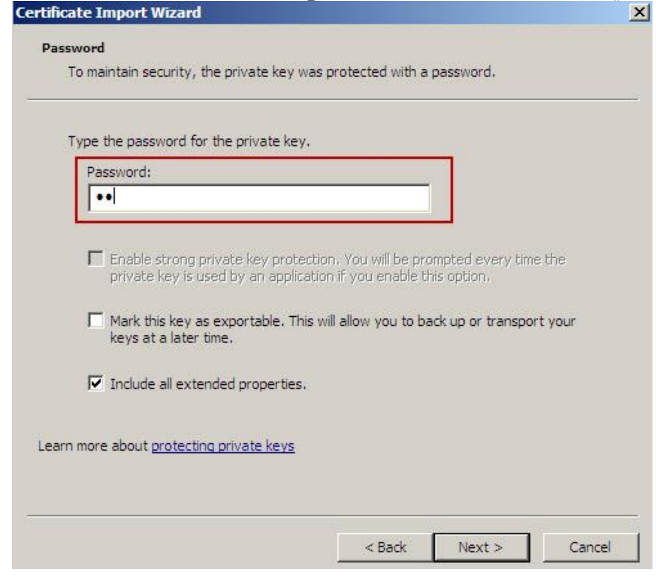


ونحدد المسار الخاص بها

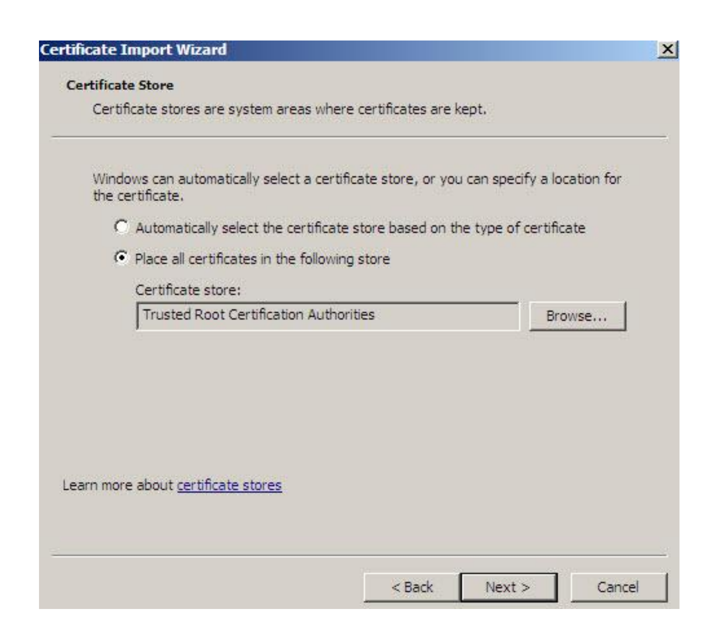




سيتم السؤال عن كلمه المرور التي تم وضعها عند اجراء الExport

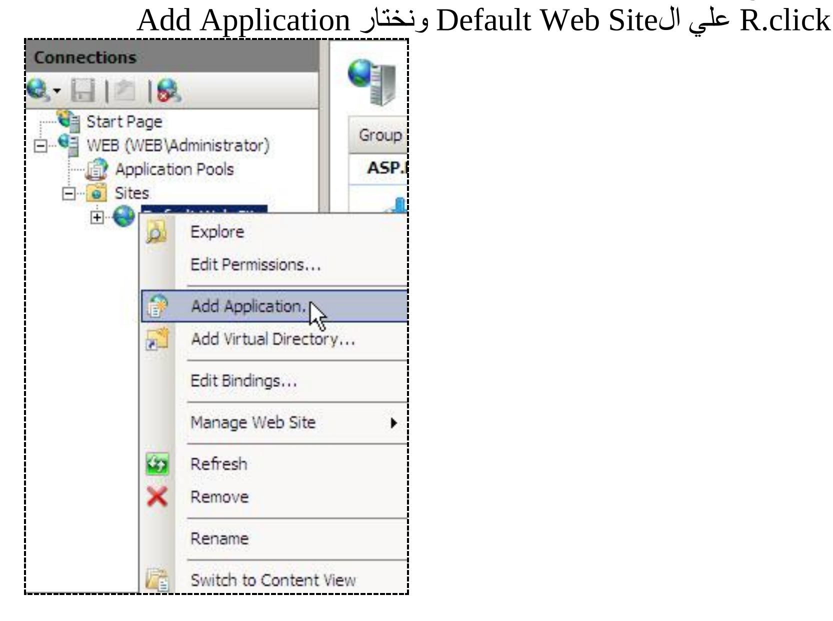


هنسيب الإختيار الثاني

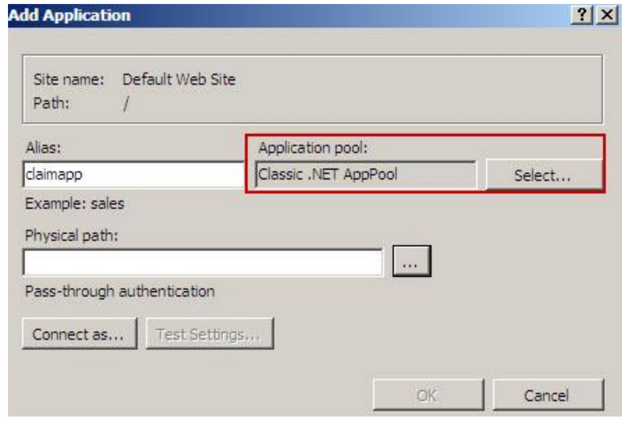




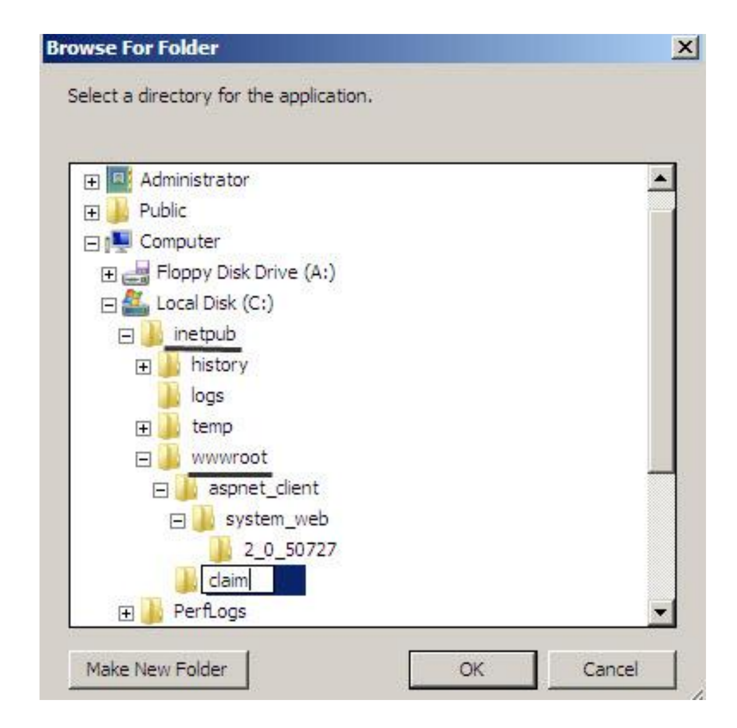
بعد ذلك نقوم بإنشاء Aware Application
نقوم بفتح الIIS
R.click علي الDefault Web Site ونختار Add Application



نقوم بتسميتها ونضغط علي Select ونختار Classic.net



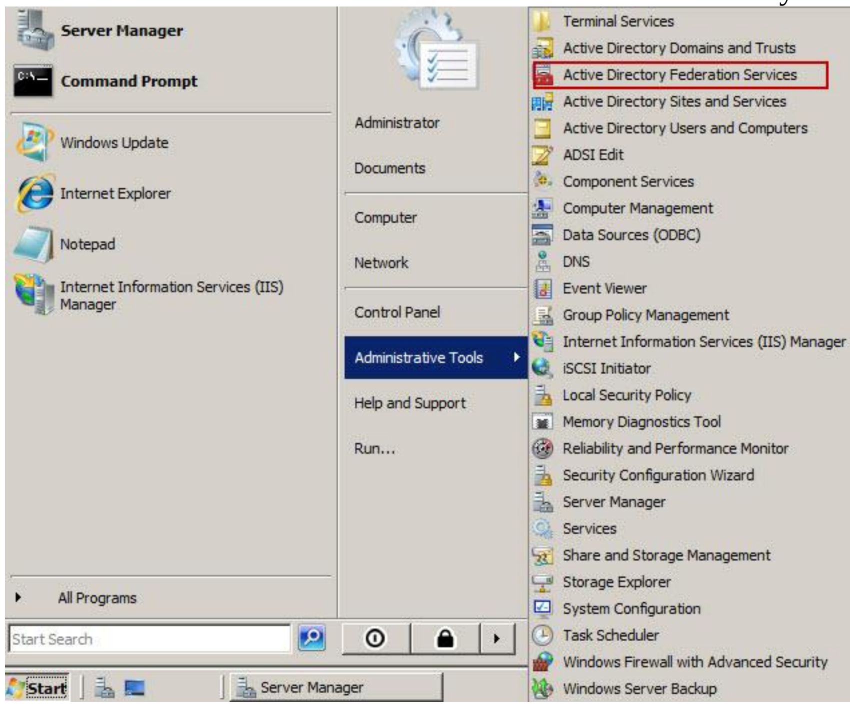
يتم حفظها في هذا المسارC:\inetpub\wwwroot\claim
ويتم انشاء ملف جديد ووضع به ملفات خاصه aware application سيتم ارفاقها مع الكتاب
مع ملاحظه انه اذا تم تغيير اي اسم من اسماء الMachine يتم تعديلها في الملف المسمي web.config



نقوم الآن بتجهيز الـFederation Service

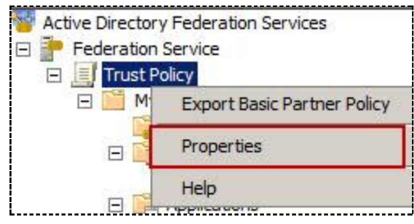
علي Ciscawy.com

Start → administrative tools → Active Directory Federation Service

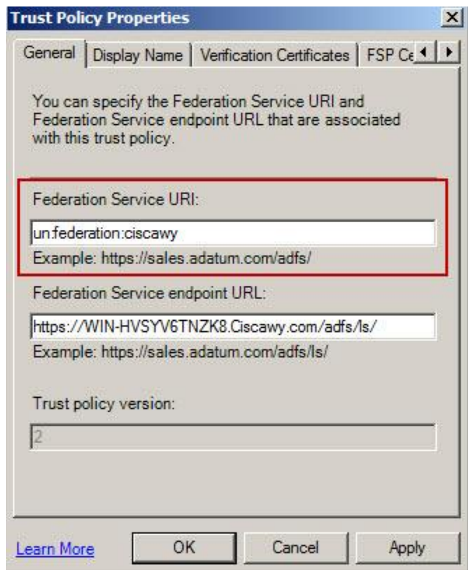


نقوم بتفعيل الـTrust Policy

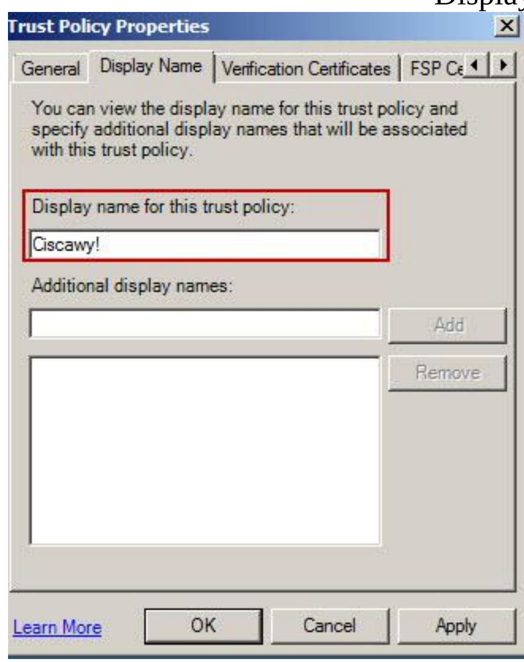
R.click on trust policy → Properties



ونقوم بتغيير الاسم الي un:federation:Ciscawy



ونقوم ايضا بالتعديل في الDisplay Name

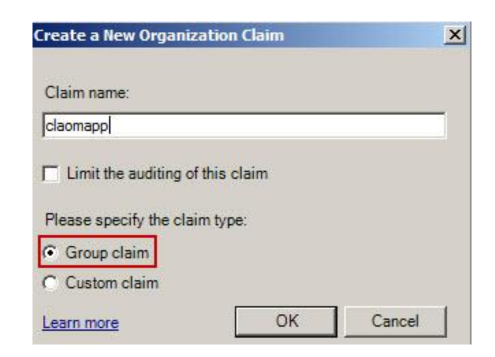


نقوم بإنشاء Group Claim التي تقوم بعمل Authentication لخدمة الFederation علي الForest الأخري

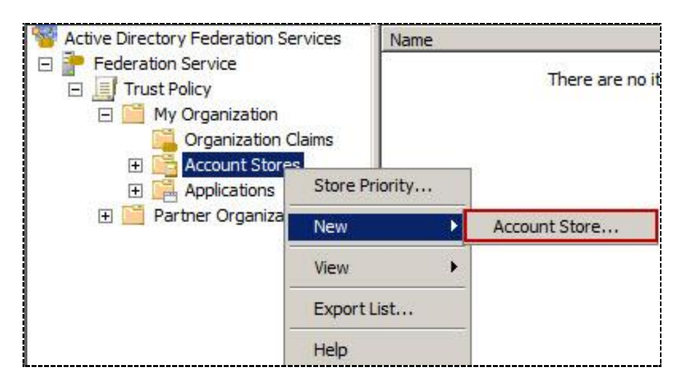
Trusted Policy → My Organization → Organization Claim

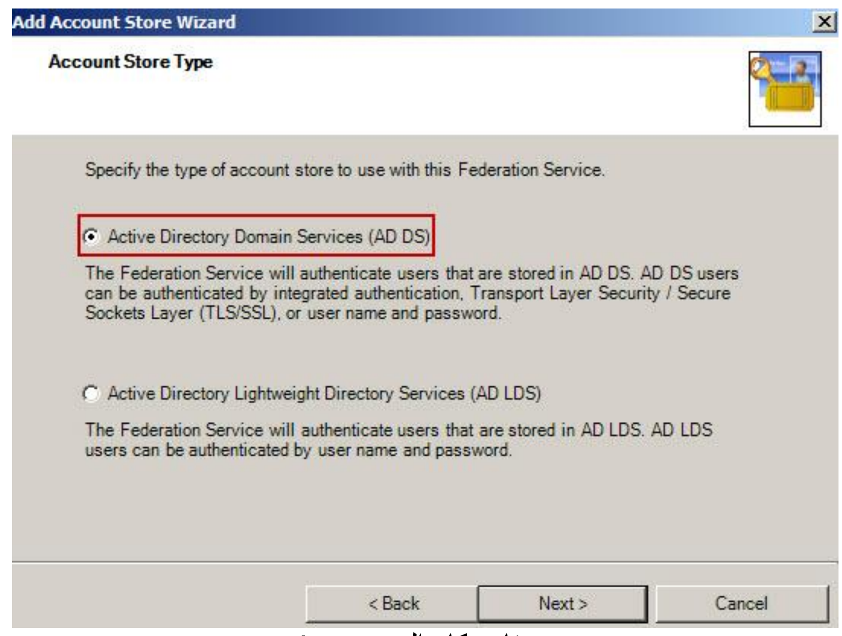
R.click → New → Organization Claim



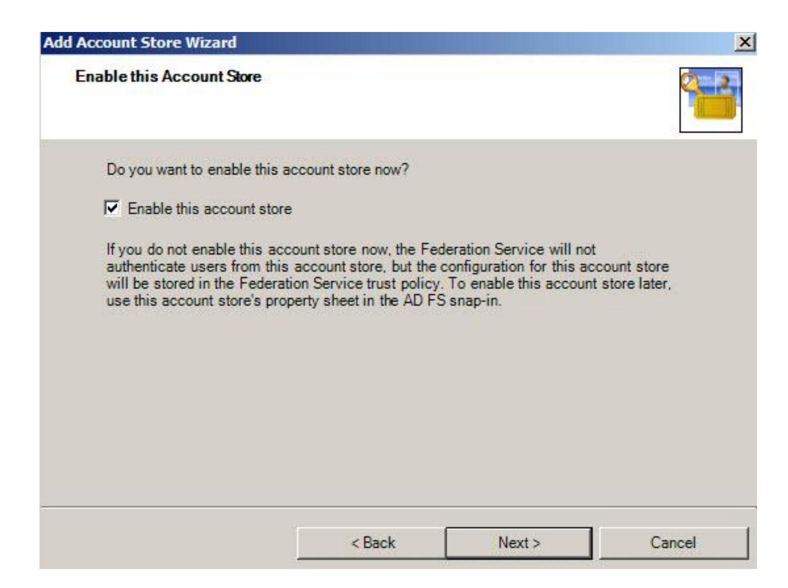


نقوم بإنشاء Account Store من الADDS حتي يتصل بالFederation Service الموجوده علي Ciscawy.com
Trusted Policy → My Organization → Account Store
R.click → New → Account Store



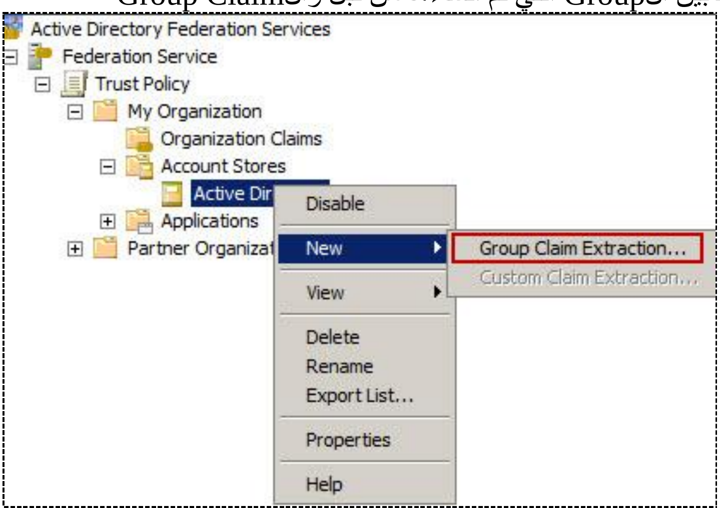


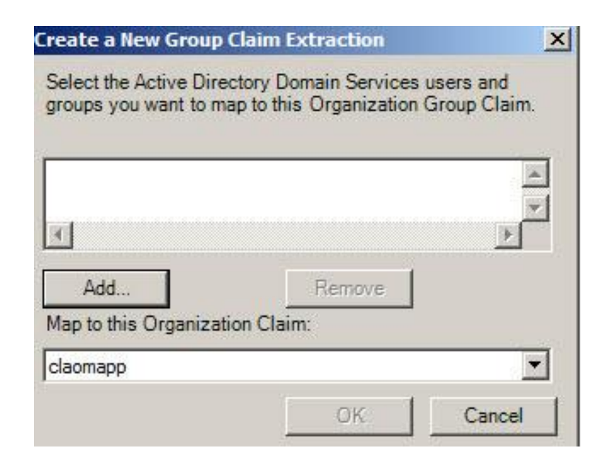
هنختار مكان الAccount
لن تستطيع ان تضيف اكثر من AD Account واحد فقط



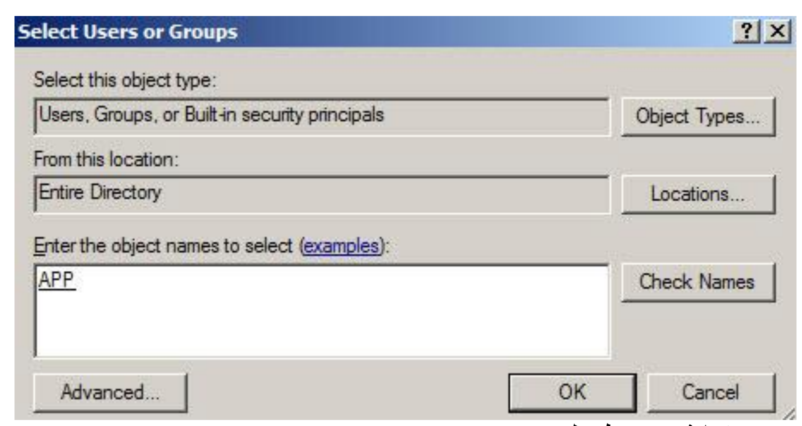
ثم نضغط علي Finish

- نقوم الآن بالربط بين الGroup التي تم انشاءها من قبل والGroup Claim





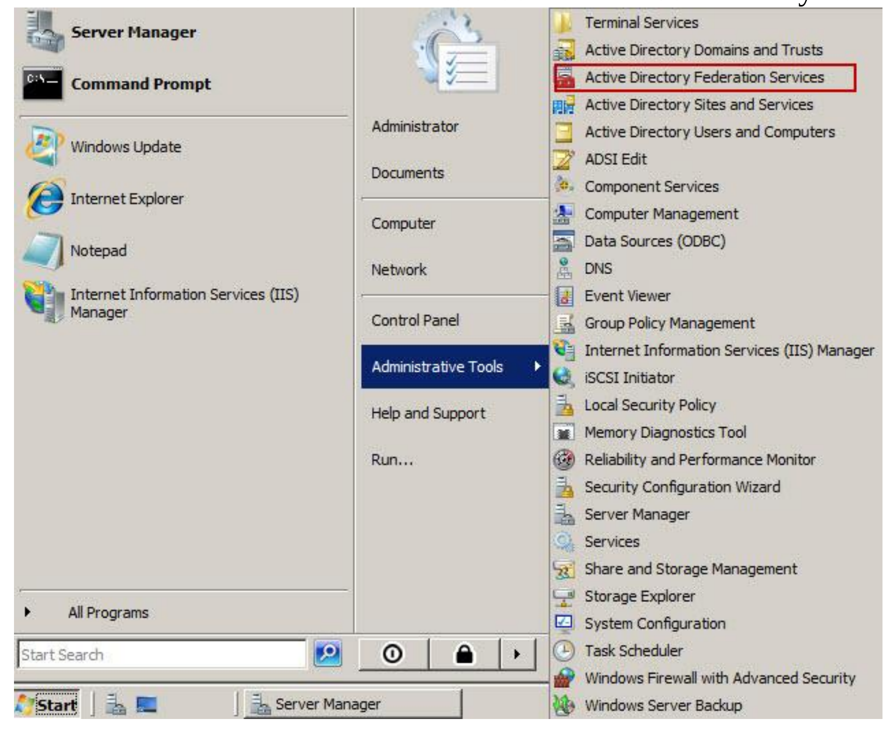
نضغط علي Add



ونبحث عن الGroup ونضيفها ثم نضغط علي ok

علي Netriders.com

Start → administrative tools → Active Directory Federation Service

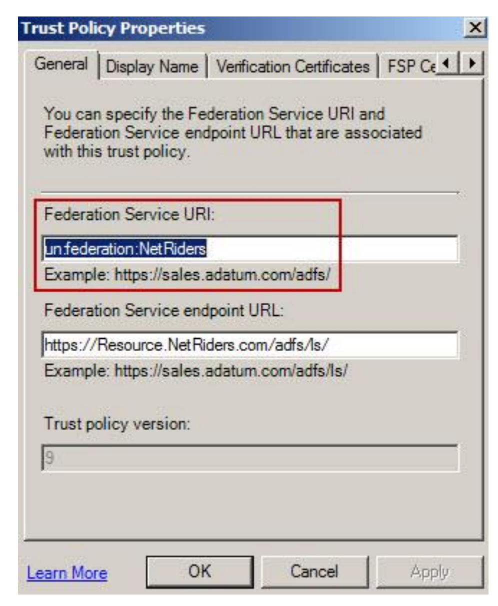


نقوم بتفعيل الTrust Policy

R.click on trust policy → Properties



ونقوم بتغيير الاسم الي un:federation:Netriders



وأيضا نعدل في الDisplay Name

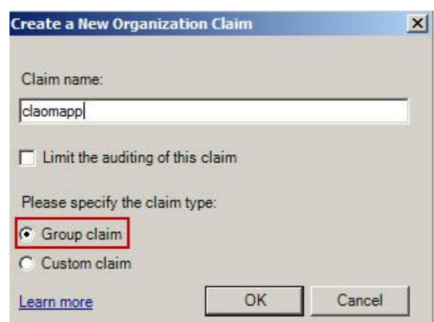
نقوم بإنشاء Group Claim التي تقوم بعمل Authorization Decision بالنسبه للApplication نيابة عن المستخدمين الموجودين في Ciscawy.com

وأيضا التي ستقوم بعمل ال Authentication في الWeb Server

Trusted Policy → My Organization → Organization Claim

R.click → New → Organization Claim





نقوم بإنشاء Account Store من الADDS

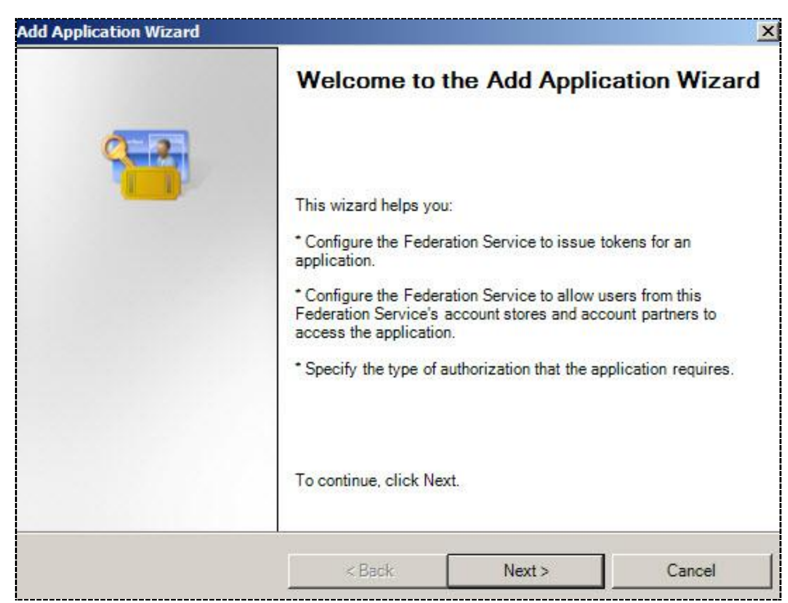
(نفس الخطوات السابقة)

ثم نقوم باضافه الApplication

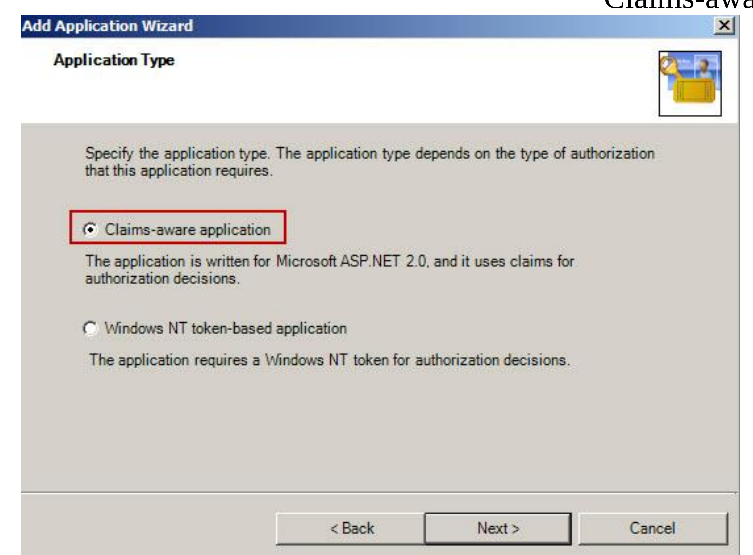
Trusted Policy → My Organization → Application

R.click → New → Application

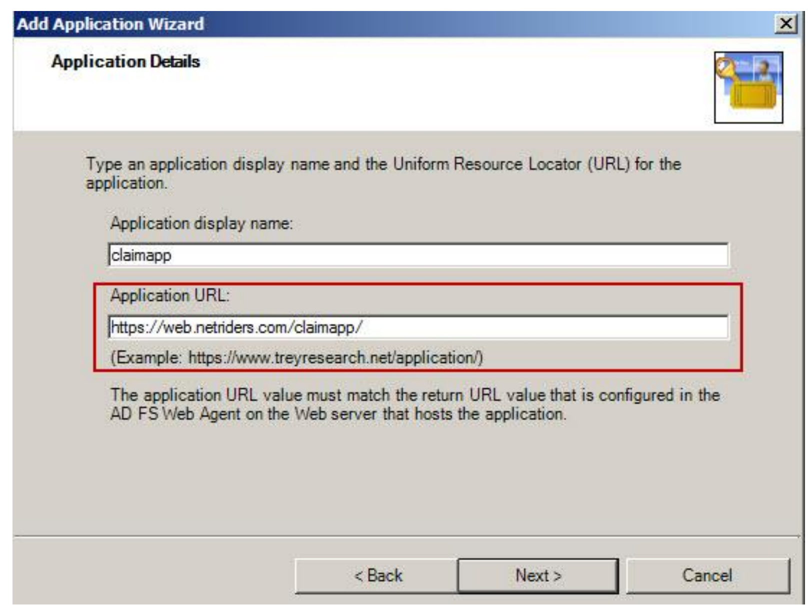




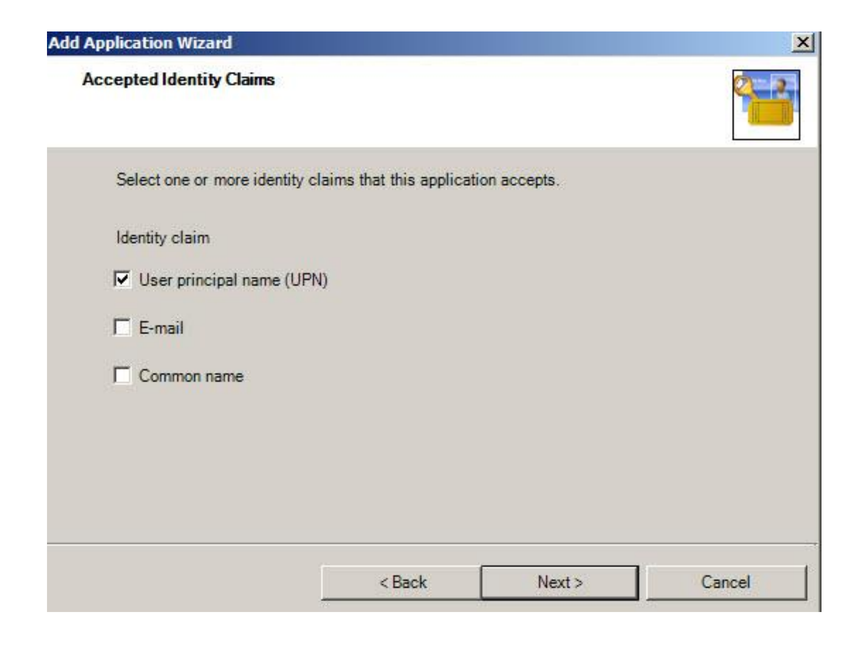
نختار Claims-aware application



نضع المسار الخاص بالWeb Server المراد الوصول إليه



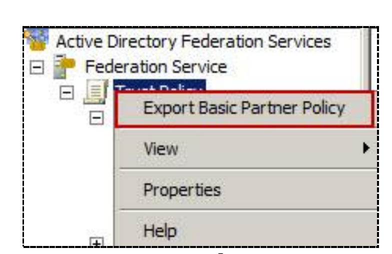
/https://web.netriders.com/claimapp
Web Serverال الموجود عليها Machineاسم ال web.netriders.com



Next → Finish

الآن سنقوم بتفعيل الTrust بين الاثنين :-
سنقوم بعمل Emport لل Policy من Ciscawy.com الي Netriders.com

علي Ciscawy.com



R.click on Trust Policy → Export Basic Policy

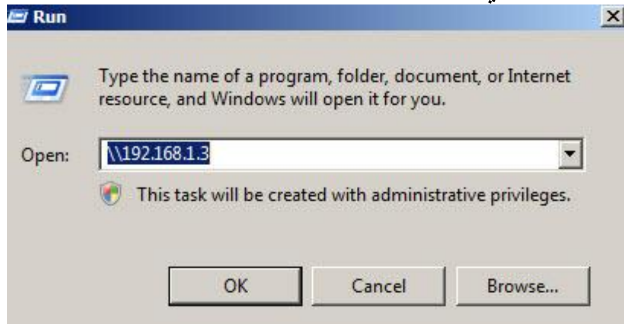


يتم حفظها في Folder

نقوم بعد ذلك بعمل Share لهذا الFolder

علي Netriders.com

نقوم بفتح المسار الخاص بالForest الاخري

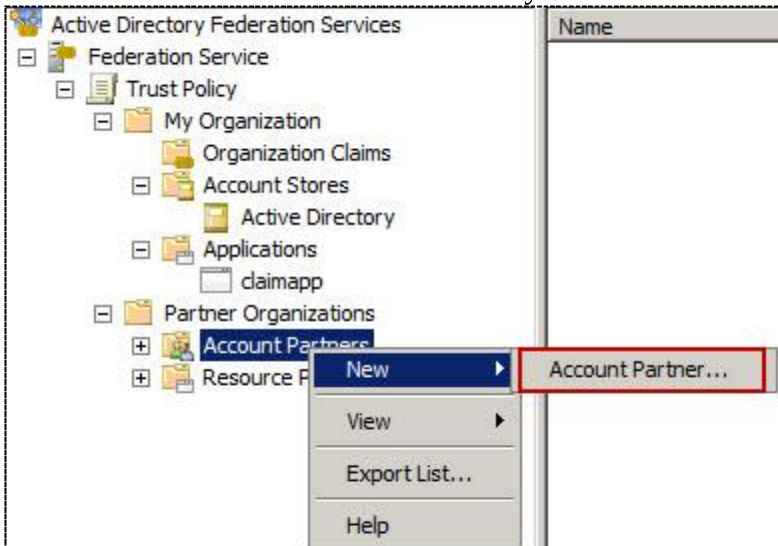


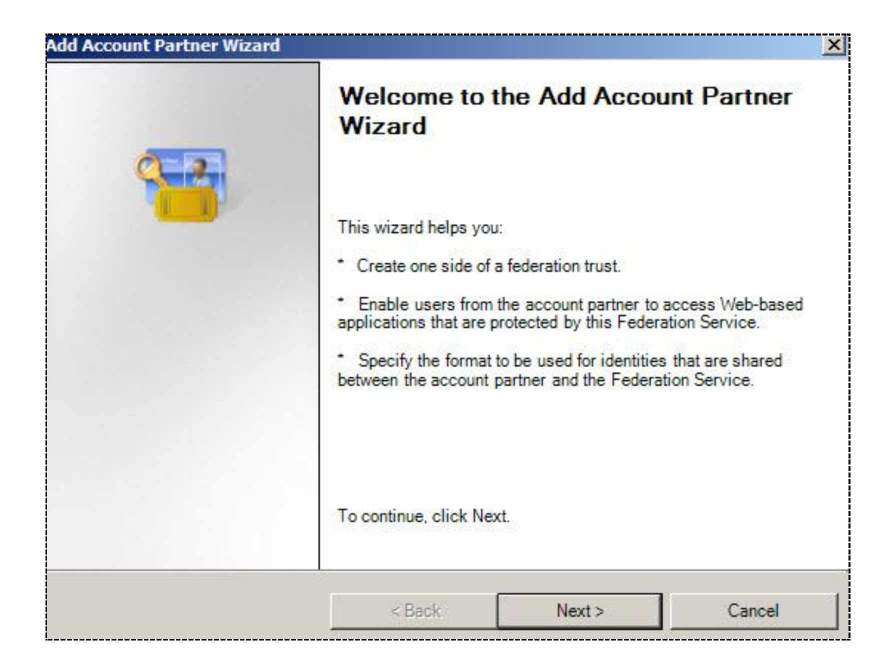
ونقوم بنسخ الPolicy علي سطح المكتب

Start → administrative tools → Active Directory Federation Service

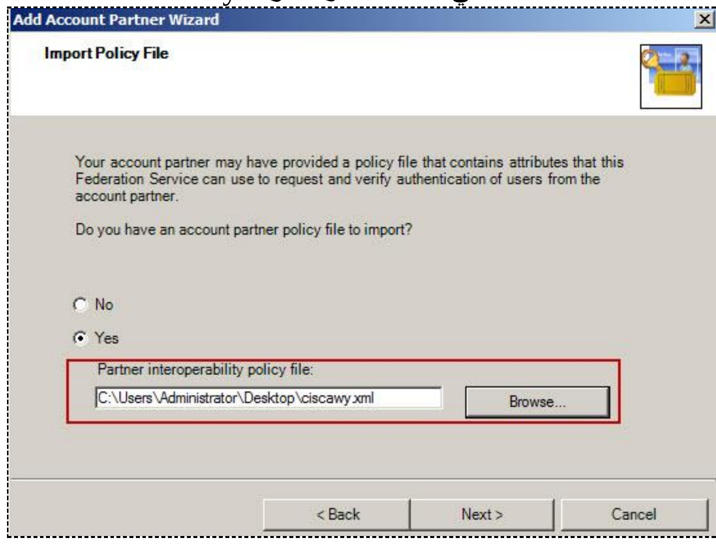
Account Partner → R.click New → Account Partner

لأن Ciscawy بالنسبه له Account

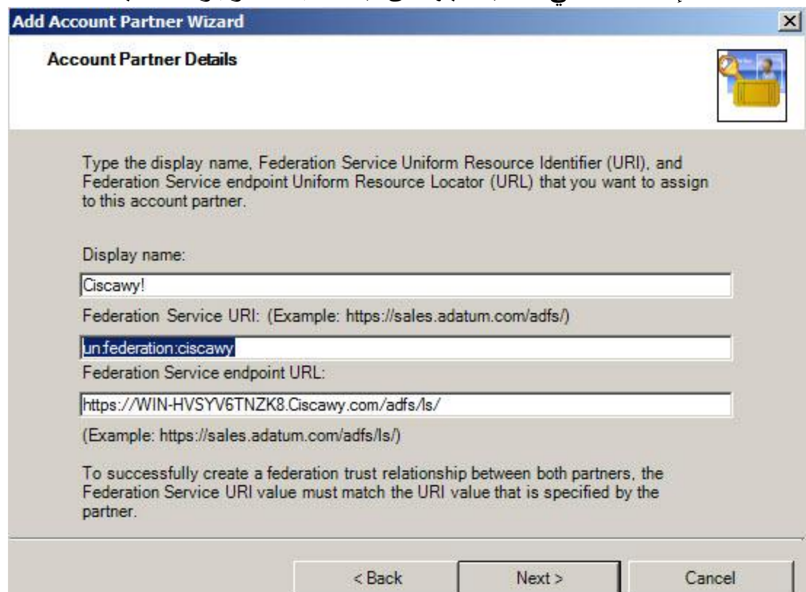


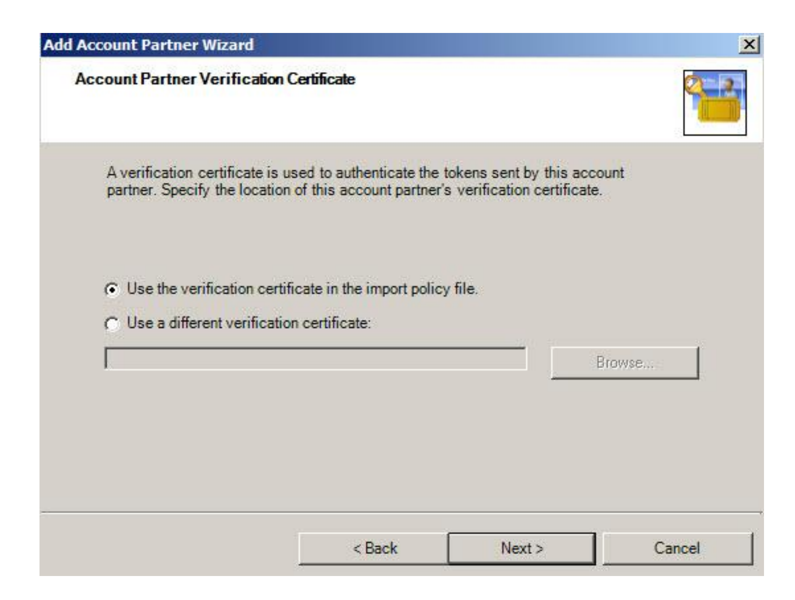


نضغط علي Browse ونختار الPolicy

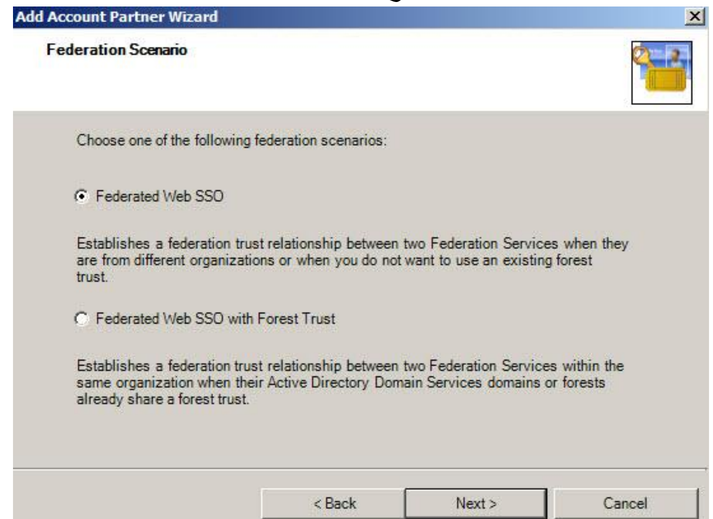


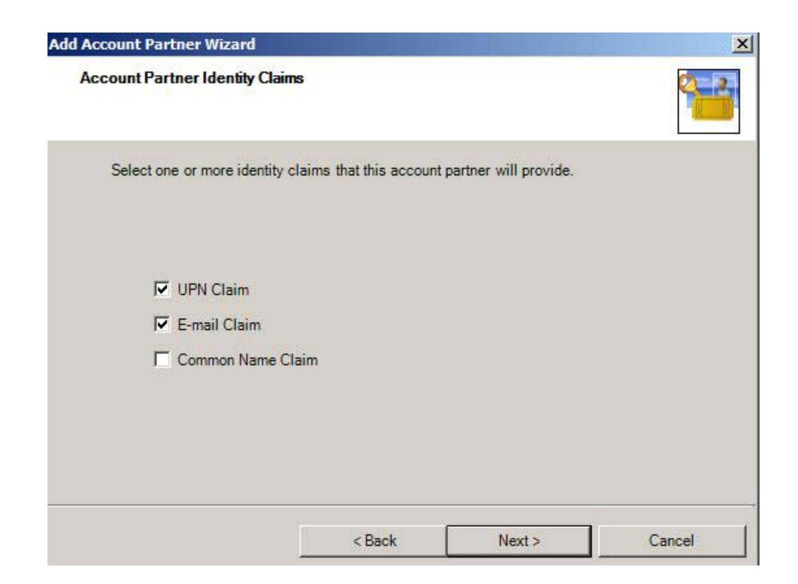
الإعدادات التي قمنا بتعديلها من قبل ستجدها موجوده تلقائيا

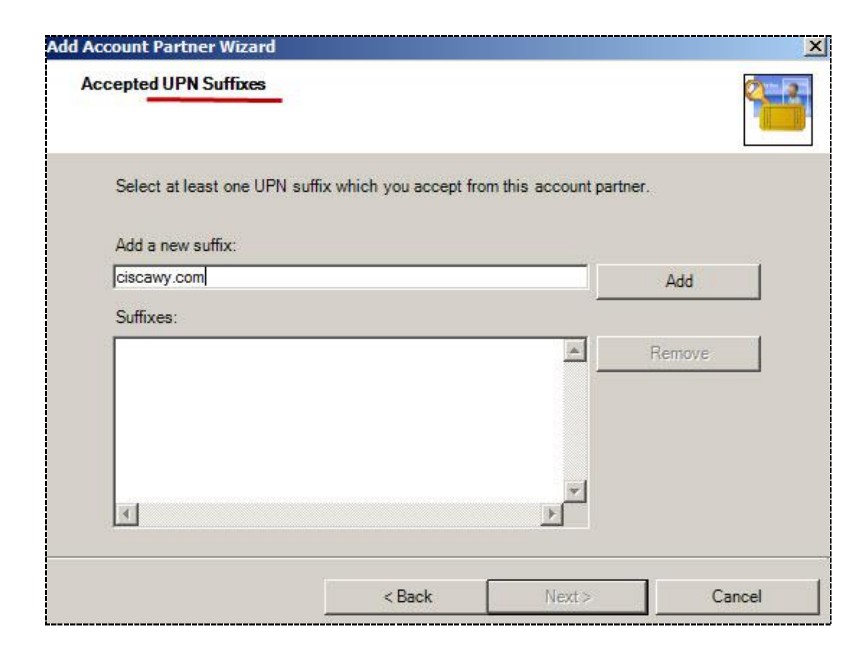


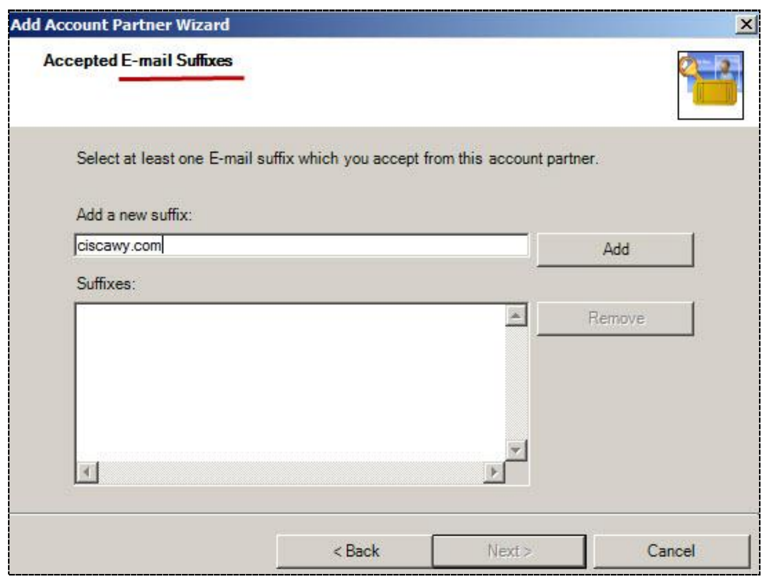


نختار SSO فقط





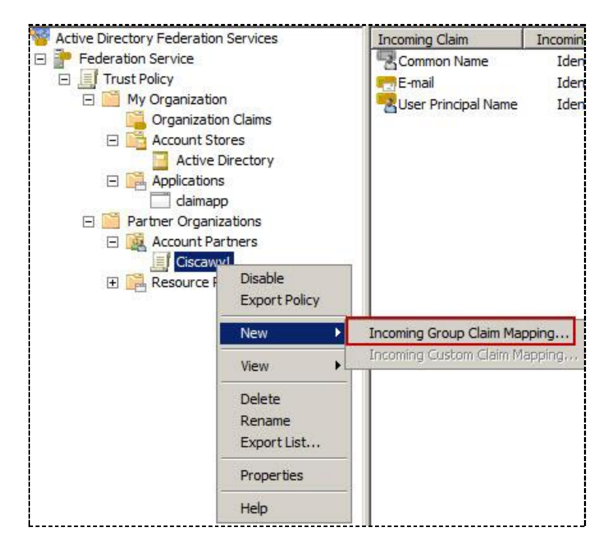


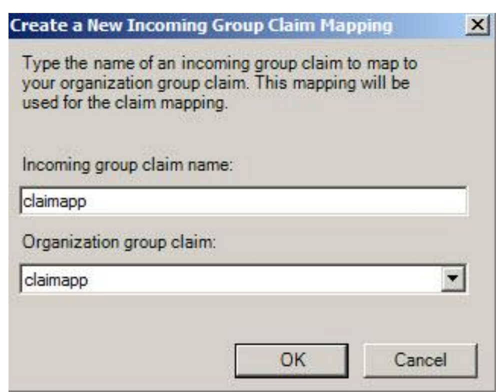


في كلاهما نكتب اسم الForest الاخري

Next → Finish

بعد الانتهاء نقوم بالضغط عليها R.click → New → Incoming Group
ستستخدم في عمليه الSimple claim aware application





سنقوم بعمل Export لـPolicy من Netriders.com الي Ciscawy.com

علي Netriders.com

R.click on Trust Policy → Export Basic Policy

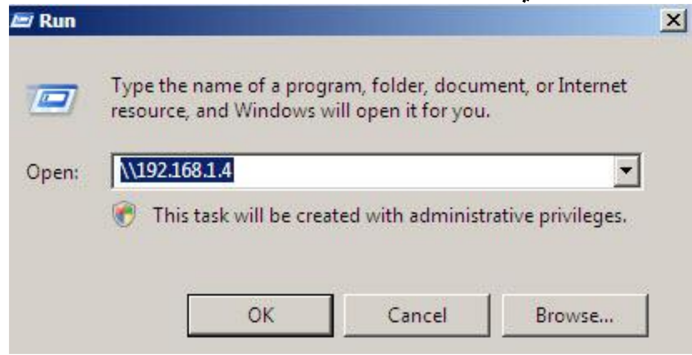




يتم حفظها في Folder

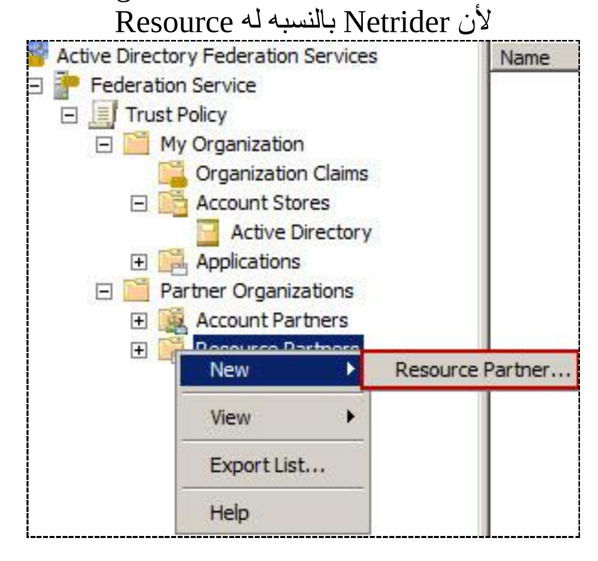
نقوم بعد ذلك بعمل Share لهذا الـFolder

علي Ciscawy.com
نقوم بفتح المسار الخاص بالForest الاخري



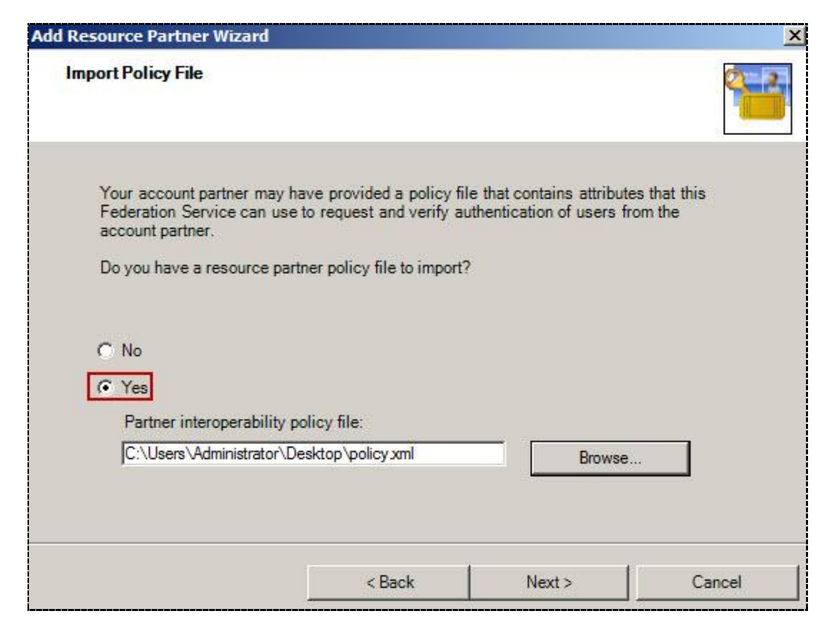
ونقوم بنسخها علي سطح المكتب

Start → administrative tools → Active Directory Federation Service Partner Organization → Resource Partner → New
لأن Netrider بالنسبه له Resource

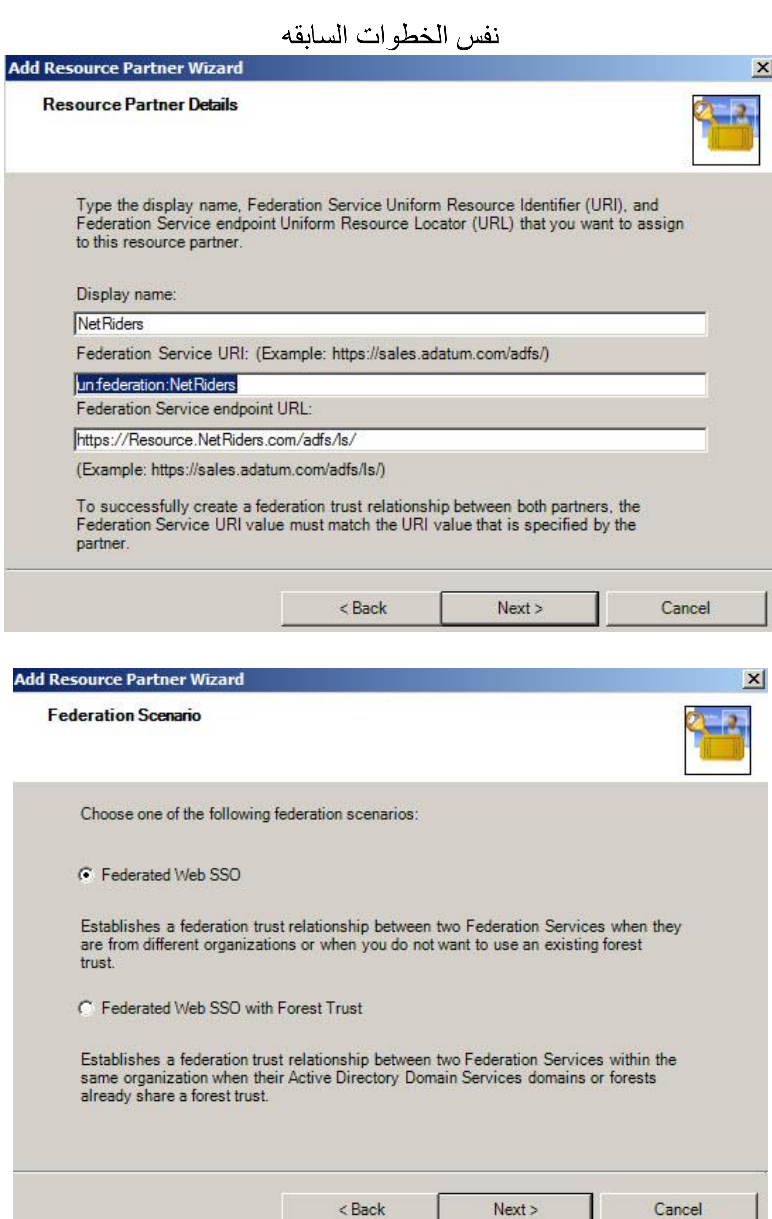


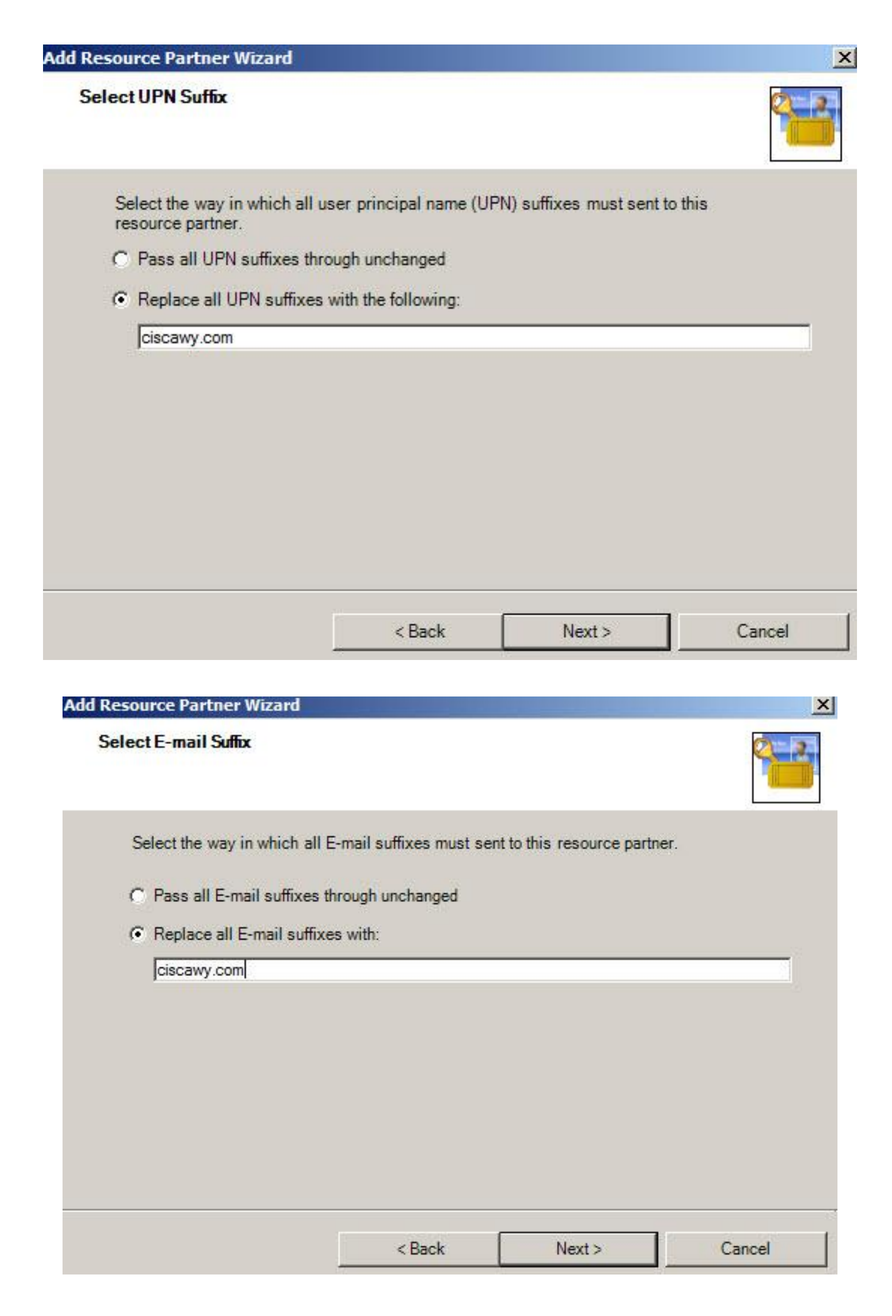


ونضيف المسار الخاص بها



نفس الخطوات السابقه





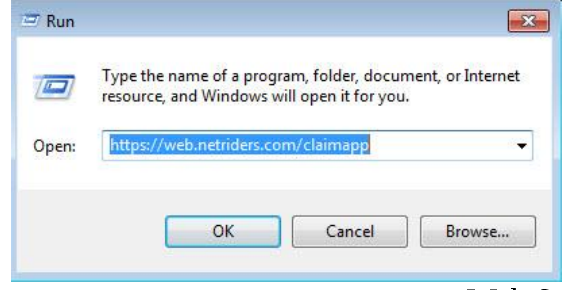
Next → Finish

بعد الانتهاء من هذا نقوم بعمل Restart للIIS (اختياريا)

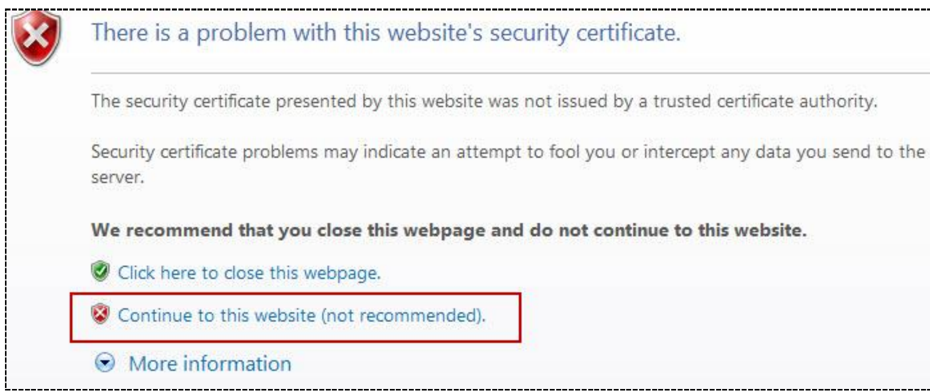
علي جهاز الClient

Start → run

https://web.netriders.com/claimapp



نقوم لفتح المسار الخاص بالWeb Server



نقوم بالضغط علي Continue

نختار الDomain الاخر !Ciscawy ونضغط علي Submit

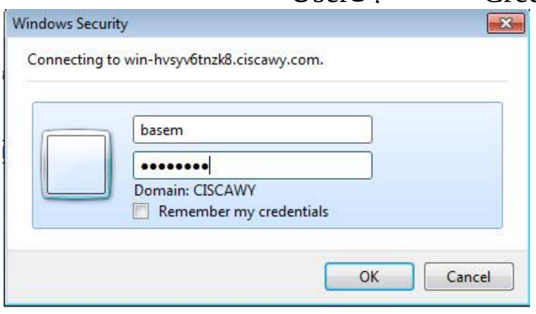
https://resource.netriders.com/adfs/ls/discoverclientrealm.aspx
DiscoverClientRealm

Choose your home realm.

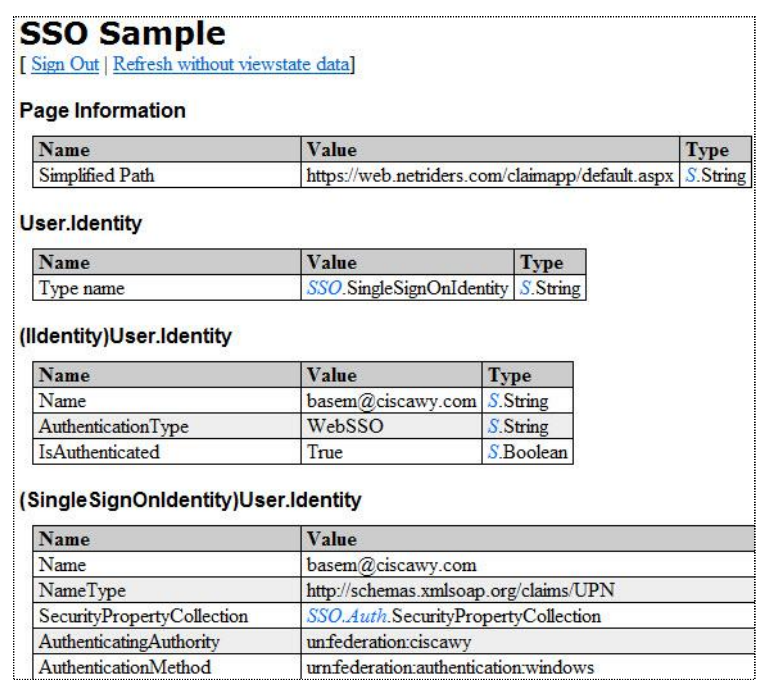
Ciscawy!

Submit

ستظهر لنا شاشه تطلب ال Credential الخاصه بالUser



ستظهر لنا هذه الشاشه
و هذه تفيد في ان الاتصال تم بنجاح



SSO Sample

[Sign Out | Refresh without viewstate data]

Page Information

Name	Value	Type
Simplified Path	https://web.netriders.com/claimapp/default.aspx	S.String

User.Identity

Name	Value	Type
Type name	SSO.SingleSignOnIdentity	S.String

(IIdentity)User.Identity

Name	Value	Type
Name	basem@ciscawy.com	S.String
AuthenticationType	WebSSO	S.String
IsAuthenticated	True	S.Boolean

(SingleSignOnIdentity)User.Identity

Name	Value
Name	basem@ciscawy.com
NameType	http://schemas.xmlsoap.org/claims/UPN
SecurityPropertyCollection	SSO.Auth.SecurityPropertyCollection
AuthenticatingAuthority	urn:federation:ciscawy
AuthenticationMethod	urn:federation:authentication:windows

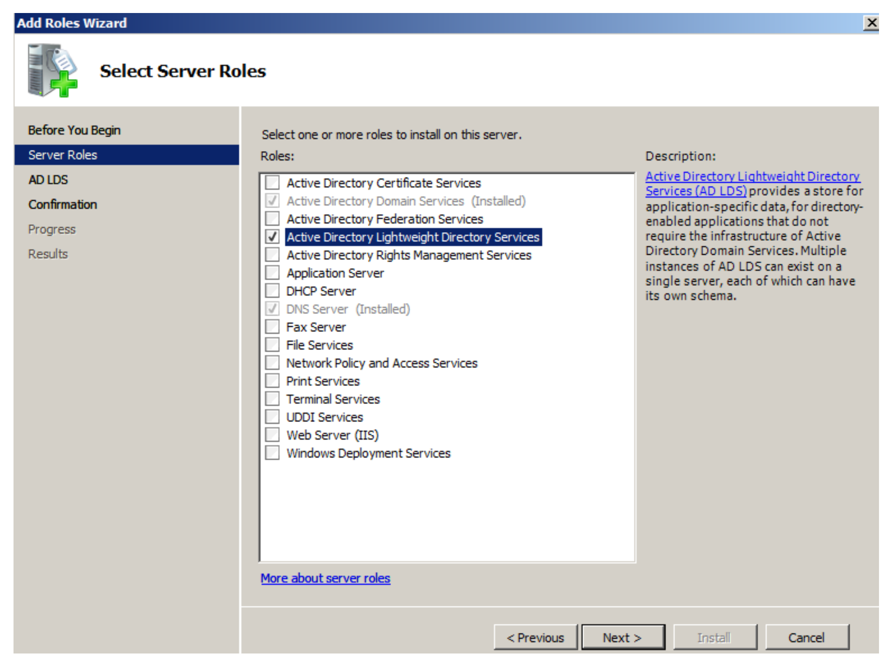
Active Directory Lightweight Directory Services

- إحدي الخدمات الجديدة في Windows Server 2008
- تتلخص فكرتها في ان هنا مبرمج او Application نحتاج تجربته علي الForest الخاصه بنا ولكن هذا البرنامج مرتبط بالActive Directory
- أي يجب ان يكون هناك Active Directory Database حتي نستطيع إستخدامه
- ابتكرت ميكروسوفت هذه الخدمه لحل هذه المشكله
- وهي ان نقوم بتنزيل هذه الخدمه علي Machine خاصه وهذه الخدمه تعتبر Active Directory ولكن أقل في الDatabase
- تعتبر نسخه Stand alone من الADDS
- امتداد لخدمه الADAM في Windows Server 2003 Active Directory Application Made
- يمكن انشاء اكثر من LDS علي نفس الMachine
- يعتمد علي الLDAP يتيح لأي مبرمج ان يتعامل مع اي Application متوافقه مع الActive Directory
- يمكن إضافته وحزفه دون الحاجه الي Reboot

- الMachine التي ستقوم بهذه الخدمه بعد تنزيلها سيكون هناك 3 Partitions
  - Schema مختلفه عن الموجوده في ADDS
  - Configuration اللي هيحصل فيه التعديلات
  - Application الموجود بها الObject ومنها يتم التعديل في الAttribute الخاصة بكل User

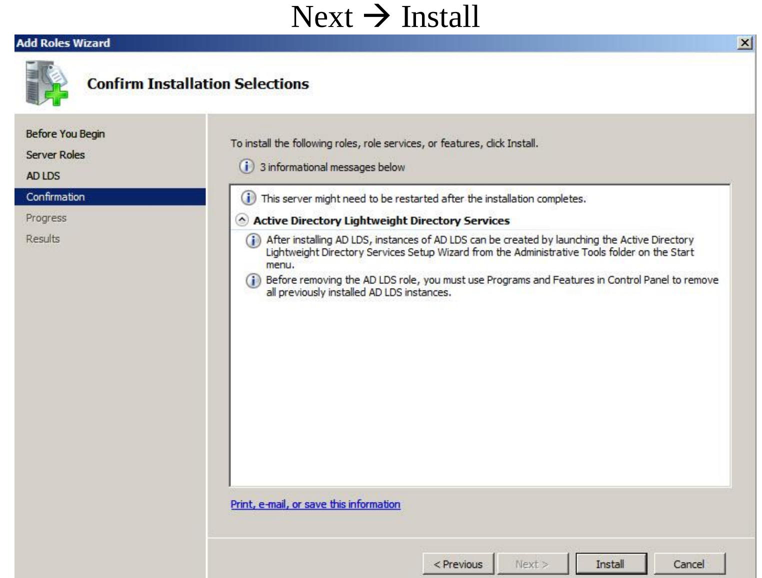
- لتنزيل الخدمه

Server manager →Roles → add role

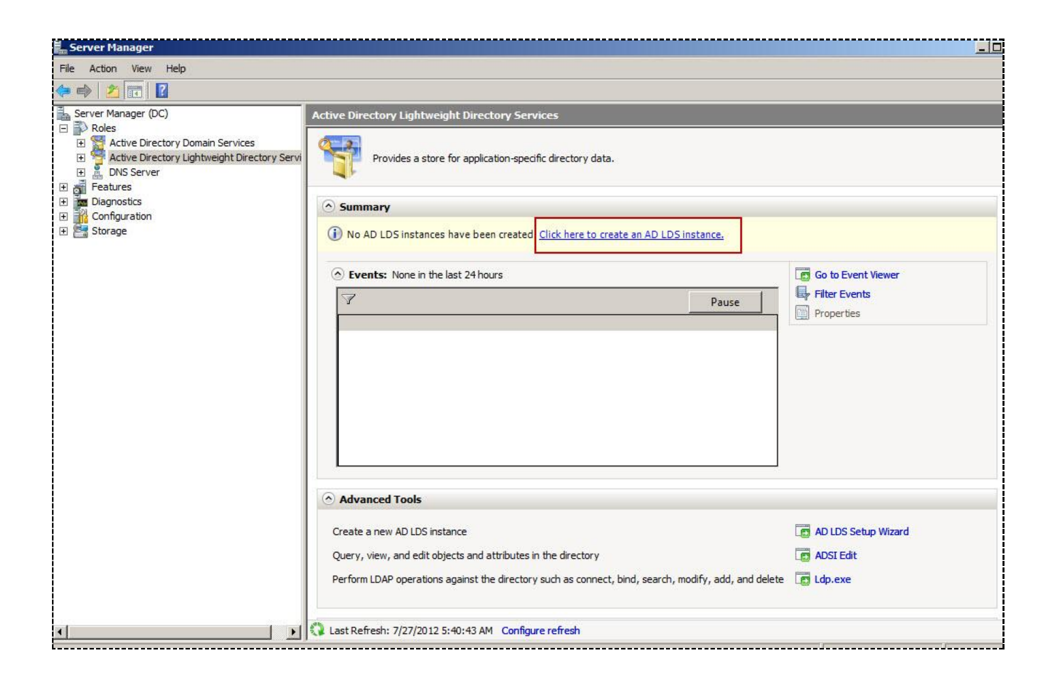


ونختار AD Lightweight Directory Services

Next → Install

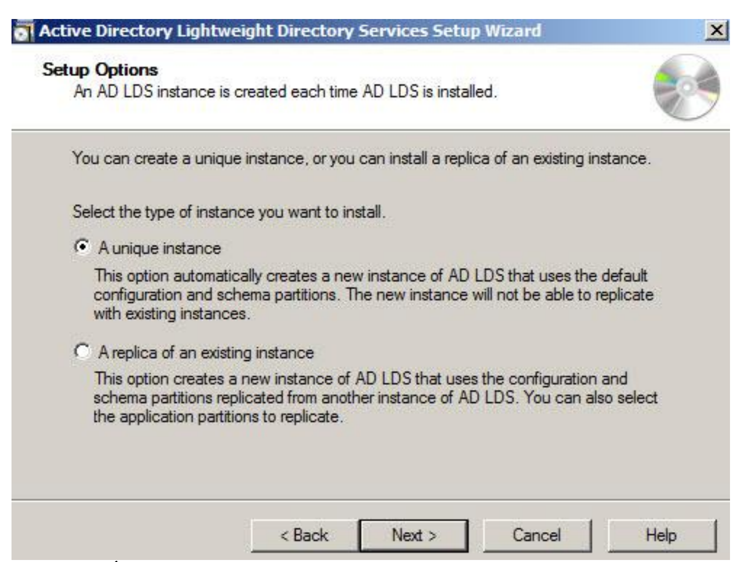


بعد الإنتهاء من تنزيلها ستظهر لنا هذه الشاشه

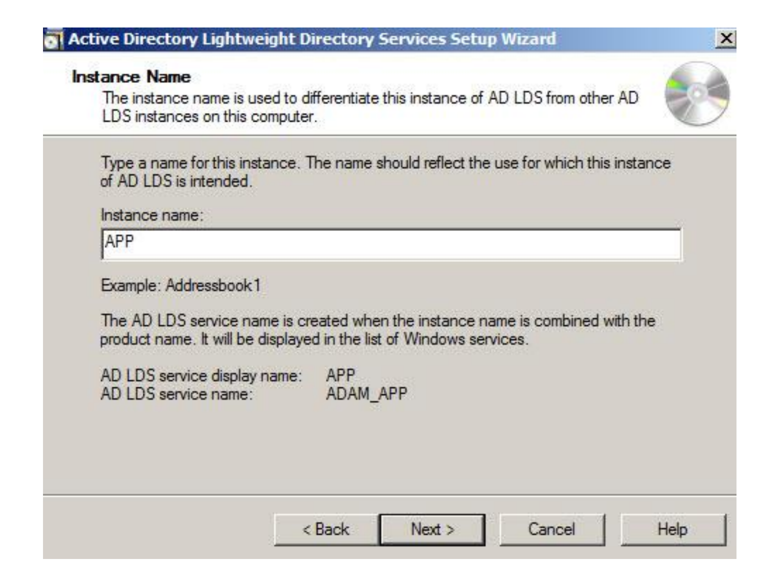


نقوم بالضغط علي Click here to create new AD LDS instance





هنختار Unique Instance عشان احنا اول مره ننشأها
ونقوم بتسميتها





لأن هذه الMachine تلعب دور الDS فإن رقم الLDAP Port محجوز ويتم استخدام ارقام اخري كما توضح هذه الصوره ان الLDAP Port الاساسي لهذه الخدمه هو 389 ولكن هذا الPort مستخدم



هننشأ Application Partition ونضيف له اسم كما هو موضح

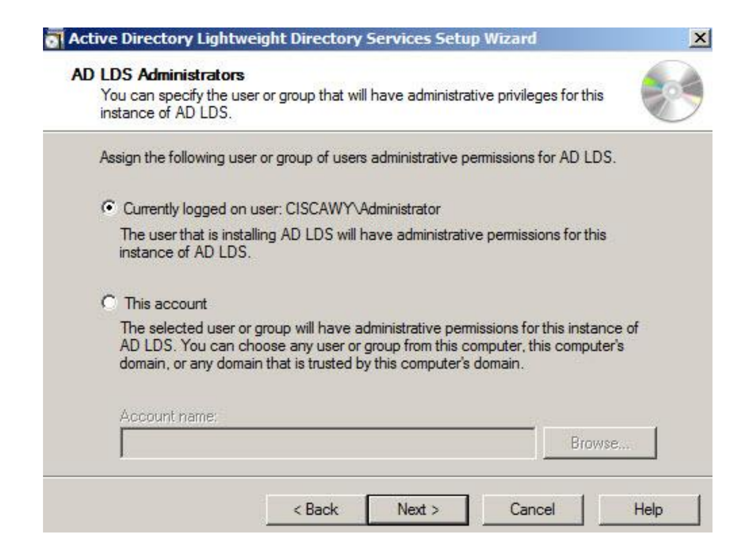
اسم الPartition وبعدها اسم الDomain

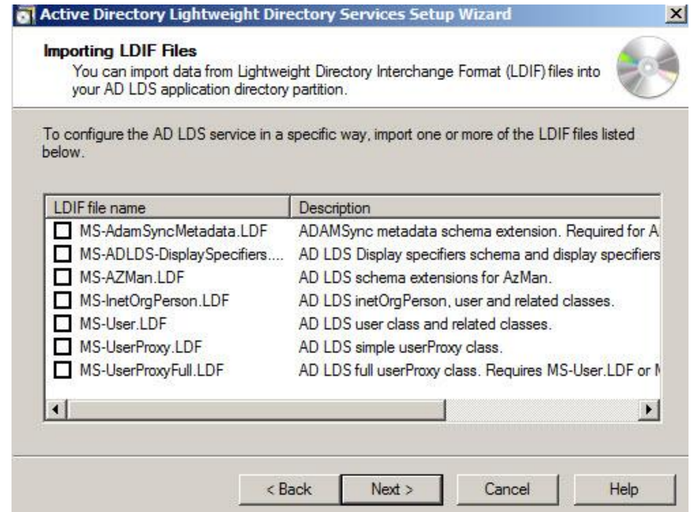


مكان حفظ ملفات ال Install

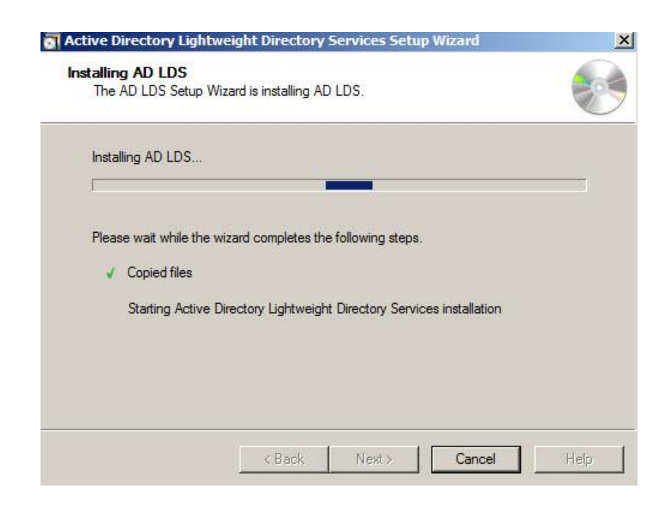


هنستخدم الDefault ولو أردت ان تسمح لUser معين استخدام هذه الخاصيه تختار الاختيار الثاني This Account وتضيفه



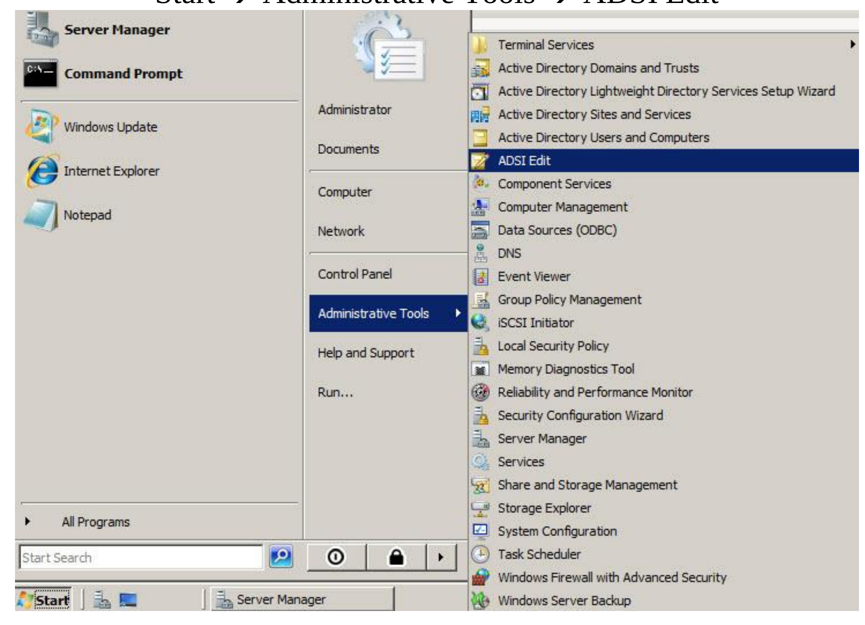


هنا يمكن ان تختار احدي الخصائص التي سيتم التعامل معها او تختارهم كلهم

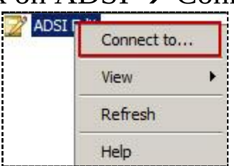


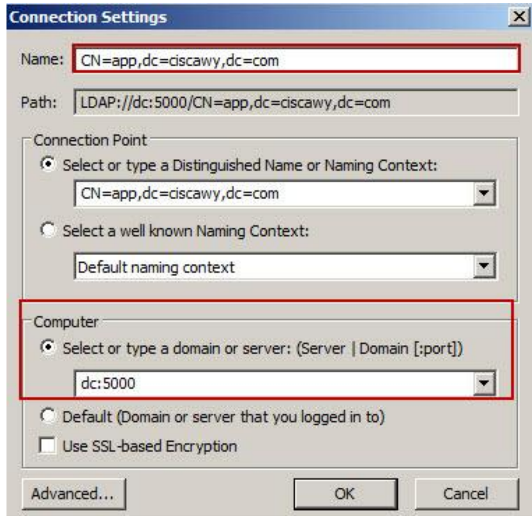
حتي نستطيع ان نقوم بفتح ال LDS :-

Start → Administrative Tools → ADSI Edit



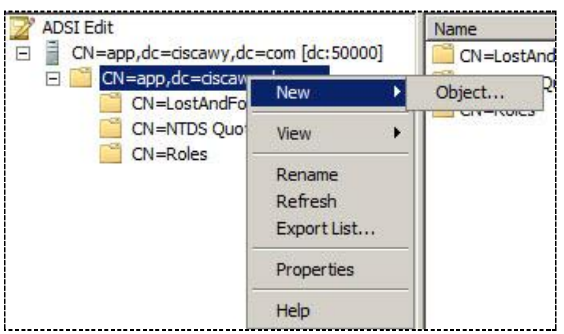
R.click on ADSI → Connect to





في الجزء الخاص بـComputer يتم كتابه اسم الMachine ورقم الPort

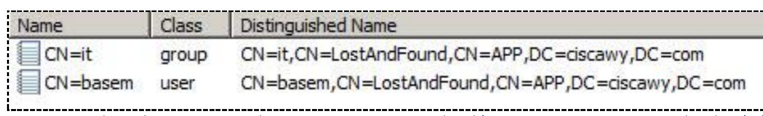
نقوم بإضافه اسم الPartition الذي أنشأناه
ونضيف رقم الLDAP Port ونضغط علي OK



نقوم بفتحها ونضغط R.click ومنها New → Object
ونضيف أي Object



نقوم بإنشاء اي Object علي هذا الServer



Name	Class	Distinguished Name
CN=it	group	CN=it,CN=LostAndFound,CN=APP,DC=ciscawy,DC=com
CN=basem	user	CN=basem,CN=LostAndFound,CN=APP,DC=ciscawy,DC=com

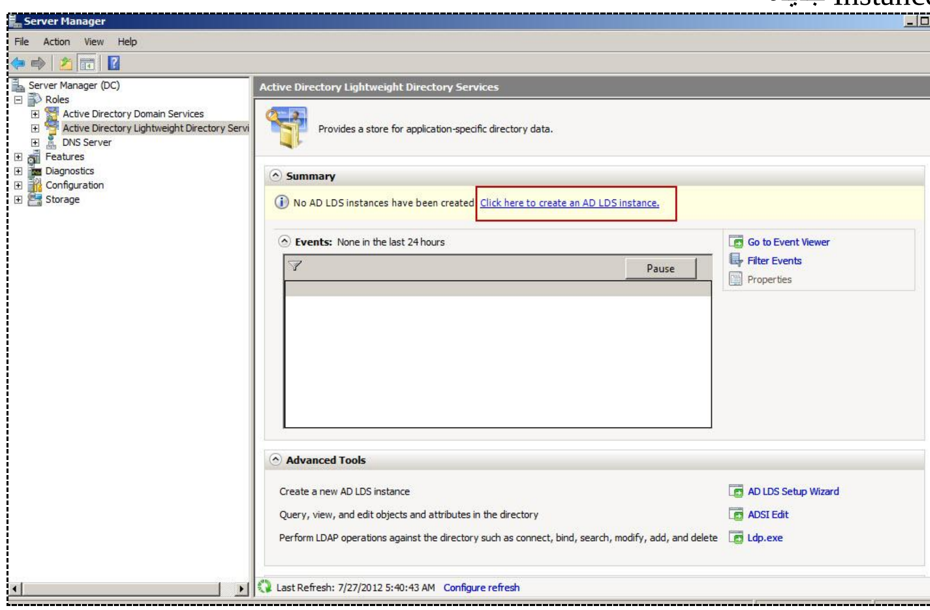
لتفعيل الReplication ونقل الInstance من الLDS 1 الي الLDS 2

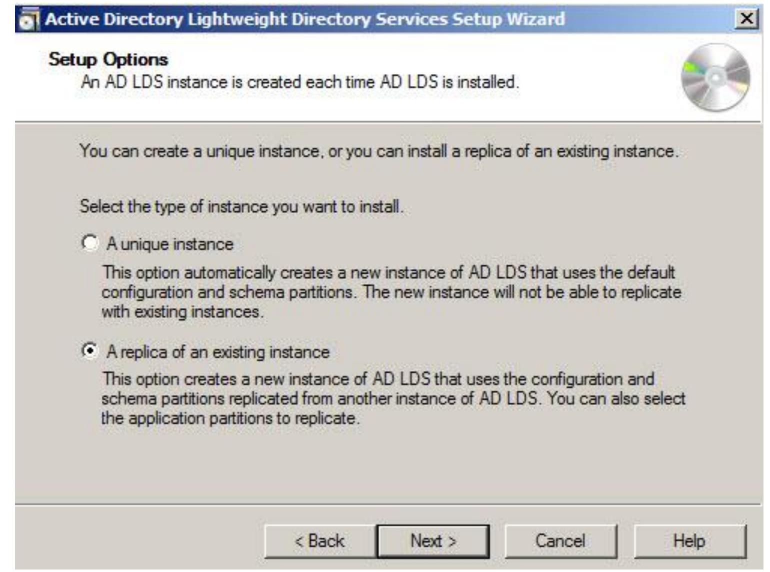
- لا تعمل خاصيه الReplication في بيئه الWorkgroup تعمل فقط في بيئه الDomain
- نقوم بتنزيل خدمه الAD LDS علي Machine أخري وتكون هذه الMachine ← Joined في الDomain الرئيسي

لأن الAD يقوم بعمل الFrame Work

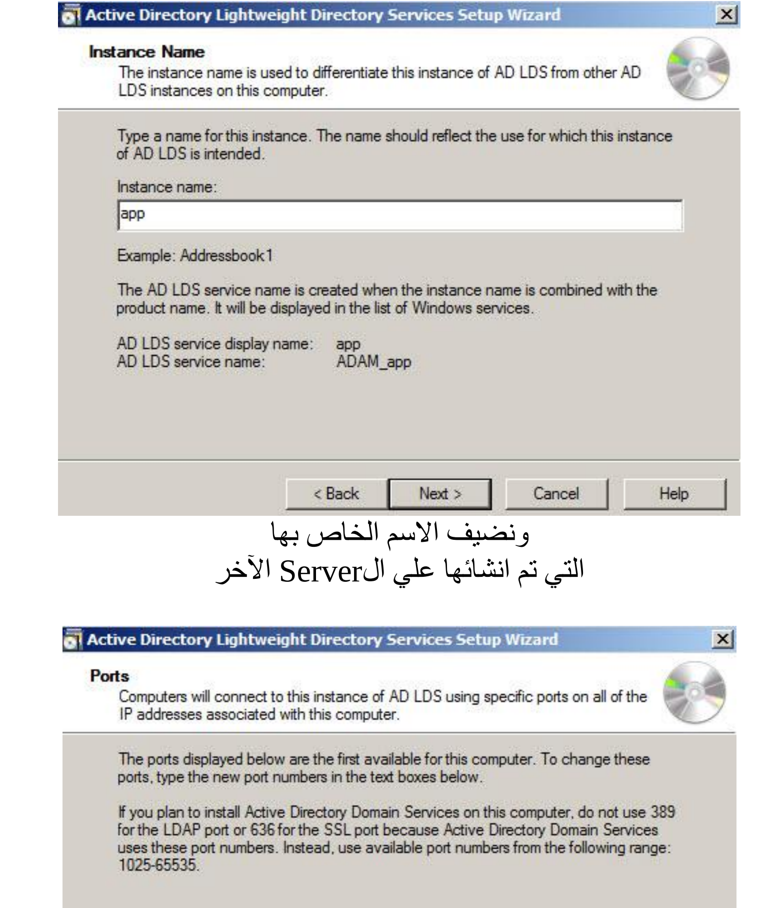
- يجب ان نقوم بفتح الPort Number في جهاز الUser من الFirewall الخاص به حتي لا يحدث اي مشاكل في الاتصال
- الوقت المخصص للReplication هو 15 ثانية
- وأي شئ سيتم انشاءه في احداهما ستضاعف في الآخر

ثم نقوم بإنشاء Instance جديده





هنختار A replica instance

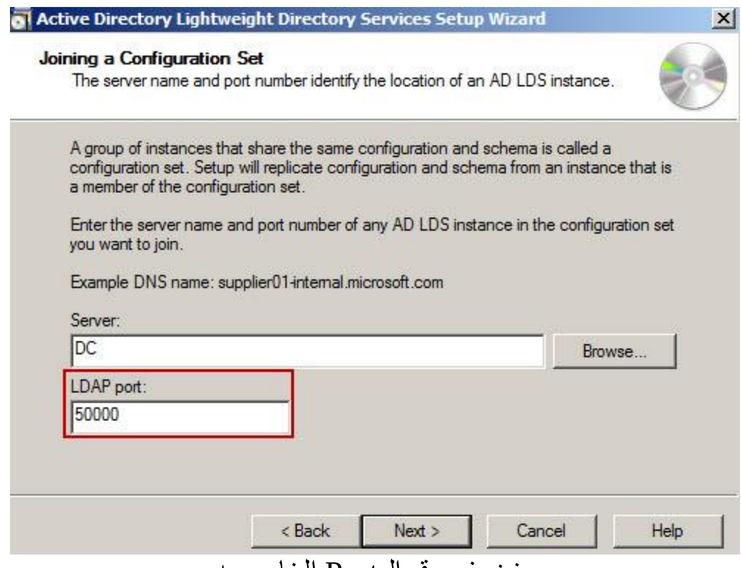


ونضيف الاسم الخاص بها
التي تم انشائها علي الServer الآخر

سنجد هنا انه أخذ الLDAP Port Number الاساسيه له لأن هنا ليس Domain Controller



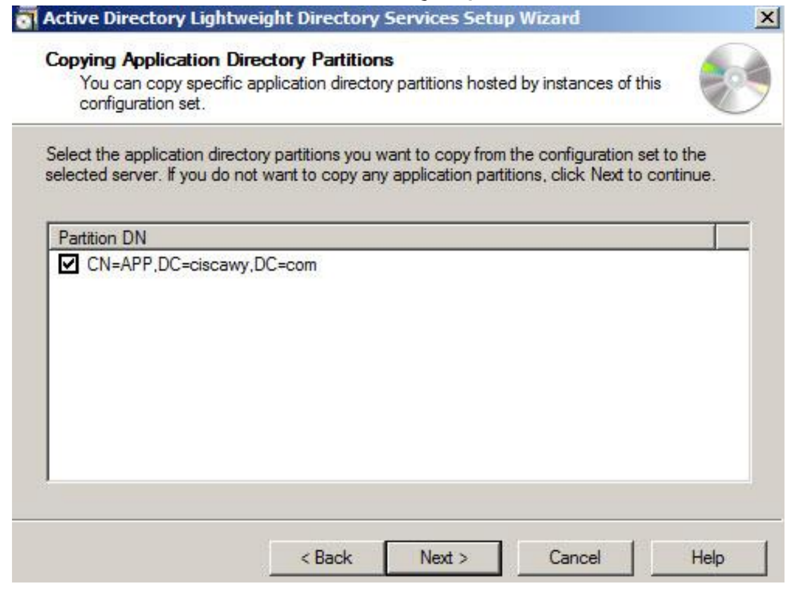
نضغط علي Browse ونختار الDomain الرئيسي الخاص بنا

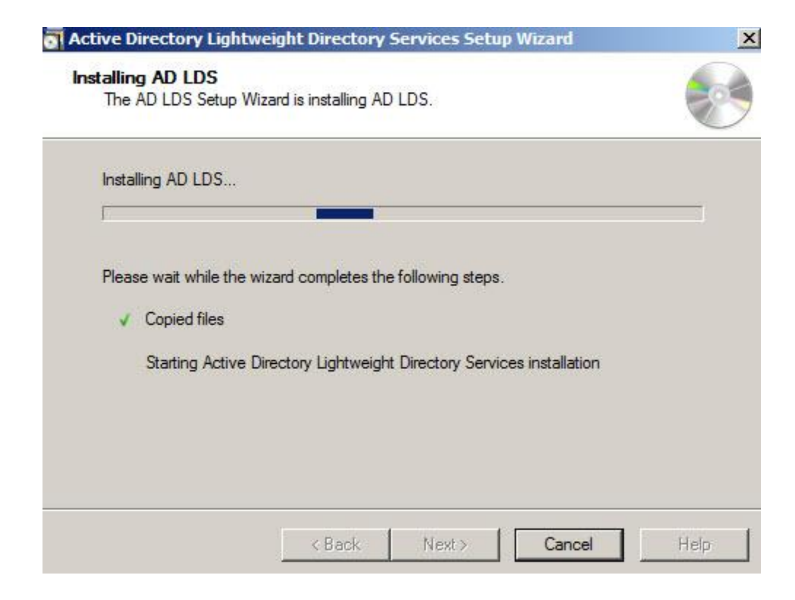


ونضيف رقم الPort الخاص به



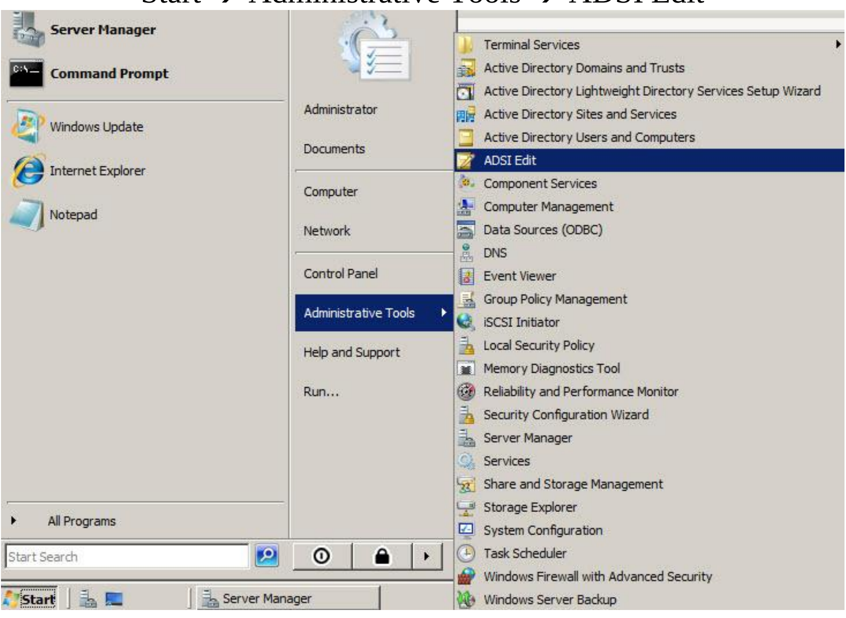
سنجد انه اتصل به وظهرت الInstance المنشأة عليه





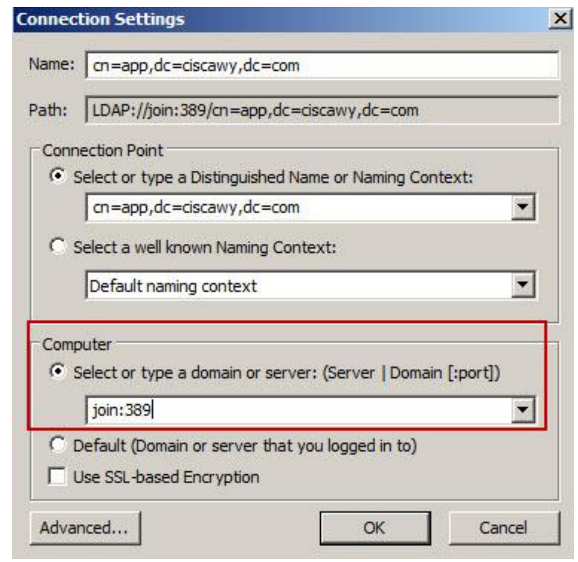
بعد الانتهاء من الInstall نقوم بفتح الAD LDS كما فعلنا علي الServer الرئيسي

Start → Administrative Tools → ADSI Edit

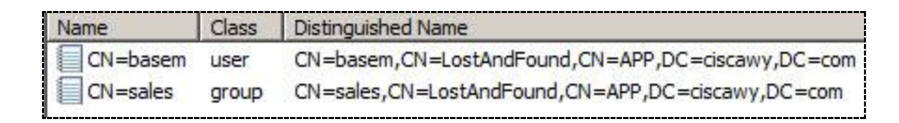


R.click on ADSI → Connect to





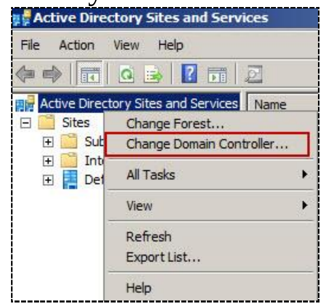
سنجد ان الObjects التي تم انشاءها موجوده بالفعل



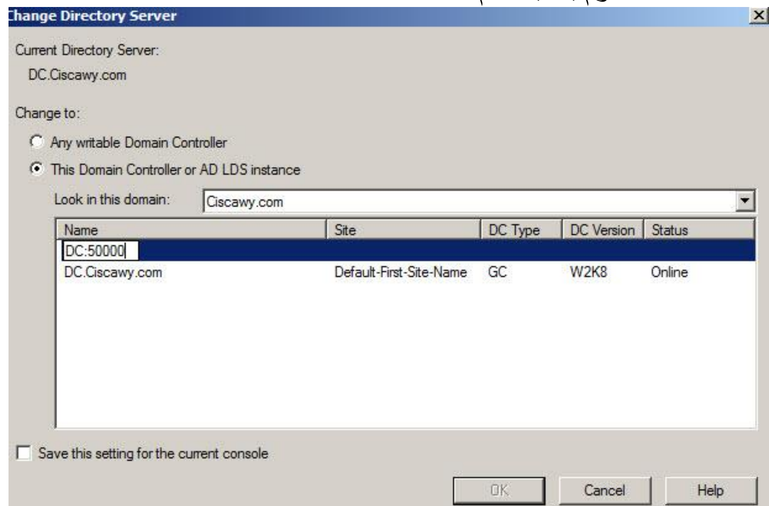
Name	Class	Distinguished Name
CN=basem	user	CN=basem,CN=LostAndFound,CN=APP,DC=ciscawy,DC=com
CN=sales	group	CN=sales,CN=LostAndFound,CN=APP,DC=ciscawy,DC=com

في حالة اذا اردت ان يكون كل منهما في فرع منفصل ويحدث الReplication بين الفروع :-

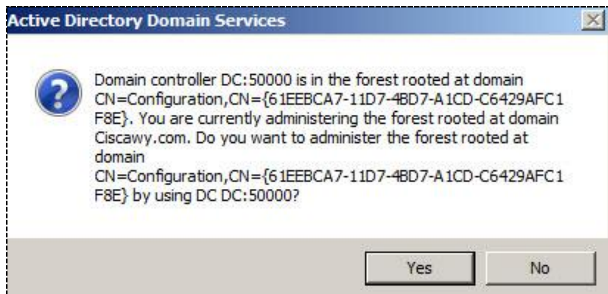
نقوم بفتح Active Directory Sites and Services



نقوم بكتابه اسم الMachine : Port number



ستجد ظهور كلمة Online بجواره
و هي تفيد ان هناك اتصال و لا توجد مشاكل



تفيد هذه الرساله انه يسقوم بفصل الاتصال عن الSite الحالي
ويقوم بالاتصال بالSite الخاص بالLDS



ستظهر هذه الشاشه
ومنها يمكن ان تنشأ Site جديد وتضع فيه الServers
كما تحدثنا عنها في الجزء الخاص بالSites and Services

تم الانتهاء من الكتاب والحمد لله
اتمني ان تكونوا استفدتم منه واضفت لكم شيئا جديدا
لا تنسونا من صالح دعائكم
جزاكم الله خيرا

المراجع :-

- كتاب الTecknet الصادر من ميكروسوفت
70-640 TS Windows Server 2008 Active Directory, Configuring 2ND.pdf

- وايضا ال Power Point المقدم منها
70-640 Server 2008 Active Directories PPT

- وبعض الفيديوهات

وسأقوم بتنزيلها علي المدونة التابعه للشركة